

FORUM SYSTEMS INC.

---

## Forum Systems Technical White Paper

TECHNICAL WHITE PAPER

# Forum Systems XML Security Appliance

---

© Forum Systems Inc.  
40 Williams Street • Suite G20  
Wellesly, MA 02481  
Phone 781-263-5400 • Fax 781-263-5401

45 S 10000 S • Suite 415  
Sandy, UT 84070  
Phone 801-313-4400 • Fax 801-313-4401



# Table of Contents

*Executive Summary* ..... 2

*The Business Integration Landscape*..... 3

**Business-To-Business Integration** ..... 3

**Internet Security Requirements**..... 3

**Value Proposition of a Dedicated Appliance** ..... 4

**The Role of XML Security** ..... 5

        XML Encryption: Confidentiality and Data Integrity ..... 6

        XML Digital Signatures: Authentication ..... 6

        XML Authorization: Access Control ..... 6

        XML Validation: Well-Formed Data ..... 6

        Next Generation XML Security Infrastructure ..... 7

*Forum Systems Solutions – Sign, Seal and Deliver* ..... 8

*Forum Systems Appliance Subsystems* ..... 9

**Appliance ForumOS™** ..... 9

**Process Manager** ..... 10

        Namespace ..... 10

        Document Identification Engine ..... 10

        Tasks & Task Lists..... 11

**Security Manager** ..... 12

**Communications Manager**..... 13

**Network Manager** ..... 14

        Packet Capturing and Transmission..... 14

        Protocol Control Packet Handling ..... 14

**Log Manager**..... 15

**Forum XMLSec™ Administrator**..... 15

        Monitoring ..... 15

        Transaction Visibility ..... 15

        Component Management ..... 15

        System Resources ..... 16

        SSL Policies ..... 16

        Server and Network Policies ..... 17

**Forum XMLSec™ Developer WorkBench**..... 18

## Executive Summary

**This document is a technical product primer for the Forum Systems XML Security Appliance product line. For specific product features please consult the appropriate product datasheet.**

As more and more businesses move their transactions and data across the Internet they are faced with a significant security challenge - *How to guarantee the protection and security of business critical data over increasingly complex trading relationships and web services.*

## The Business Integration Landscape

### Business-To-Business Integration

For many years organizations have had the need to electronically collaborate with customers, suppliers and partners. Electronic collaboration yields significant cost savings and efficiencies in key processes such as procurement, supply chain management and cash management.

In the past there have been several attempts at creating ubiquitous standards for electronic trade; perhaps the best known is Electronic Data Interchange (EDI). EDI defines a set of message structures for different horizontal and vertical markets.

One of the problems with EDI is that in almost all cases, companies developed custom EDI message structures that are not reusable causing considerable scalability problems for organizations. Another major drawback of EDI rigid format is the high cost associated with adding new trading partners, as message structures must be negotiated *up front* for each trading partner.

The promise of XML is to allow organizations to establish a standard set of interfaces that can be used for B2B integration without negotiation. XML is becoming the most relevant standardization effort in the area of business document representation through markup languages. XML changes the way that organizations do business, because it allows them to reconfigure rather than re-implement business interfaces.

It is understood that the reader has a fair understanding of the business benefits of XML and how business integration implementations use this technology for low-cost and efficient cross-enterprise business process automation.

### Internet Security Requirements

Today, business integration implementations rely upon the Internet based technology known as Secure Sockets Layer (SSL) as the primary mechanism to secure business-to-business data exchanges. SSL provides excellent security between two entities by securing the communication channel at the packet data level. SSL does this by offering “in-transit” data confidentiality (using encryption technology) between two SSL-enabled parties. Unfortunately, while this data sits on either end of the communication link it is left completely unsecured.

Companies that send unencrypted XML data across the Internet are essentially leaving the keys to their office on the doorstep. Without a granular level of XML data security corporations are exposing critical business data to theft and tampering, as it lies vulnerable on web and application servers.

*The solution: Extend existing Internet security with technology that is specifically designed to secure Internet-based business processes.*

Internet business processes can span multiple trading partners, require interaction between many entities (users as well as machines) and integrate with corporate security policies for access control and authorization. Enterprises must implement comprehensive Internet security that is specifically designed for today's Internet business processes including:

- End-to-end confidentiality -- No one else can access or copy the data while it is stored on computers or while it is in-transit.
- Integrity -- The data isn't altered as it goes from the sender to the receiver.
- Authentication (user and data) -- The document actually came from the purported sender and is received by the intended recipient.
- Non-reputability -- The sender of the data cannot deny that they sent it, nor can they deny the contents of the data.
- Network Appliance security -- The device is designed to protect against network attacks such as denial of service

### **Value Proposition of a Dedicated Appliance**

A dedicated Appliance offers differentiated customer value by managing the complexity associated with *access to and exchange of critical business documents* in a hassle free black-box package.

A dedicated XML *Security* Appliance should enable companies to:

- Instantly deploy commodity services such as digitally signing documents, accelerated data validation and transaction logging.
- Reduce the number of costly software based "clusters" by replacing key software services with less expense hardware-based implementations.
- Bridge the Enterprise-to-Internet gap by expanding the reach of business integration outside the firewall through Internet technologies such as XML, HTTP and SOAP.
- Automate the complexity of many-to-many trading partners including individual protocols and message formats, various document grammars, tracking and acknowledging transactions and granular content-level security.

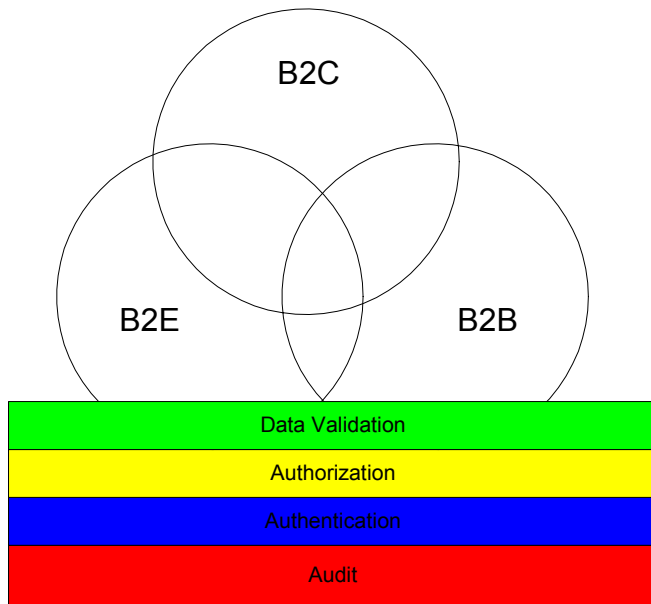
### The Role of XML Security

XML is becoming the Lingua Franca of business data representation. Through XML it is possible to define complex documents containing information at different degrees of sensitivity. While most enterprise security infrastructure focuses on internal business processes, the role of XML Security needs to be comprehensive and include Internet business processes that cover: business to consumer, business to business as well as business to employee applications.

Policies that control and regulate the access and dissemination of XML documents need to exist beyond end-point confidentiality using encryption and must also include authentication, authorization and auditing capabilities (see diagram below). In addition, the protection requirements need to be at the “content-level” applying security polices to specific portions of a document.

The next sections describe each of the key areas of XML document security.

(The use of data and document will be used synonymously throughout this White Paper).



**XML Encryption: Confidentiality and Data Integrity**

Because XML is a text based markup language end users and machines can pull information out of an XML document whether or not they have the appropriate privileges to specific data. By including content-level security within a document it is possible to have restricted information inside a document, avoiding modification of and access to sensitive information. The most basic example of the need for content-level confidentiality occurs can be highlighted during a typical e-commerce order entry transaction. In most e-commerce transactions the customer is required to provide sensitive information such as a credit card number to the merchant. This credit card information is destined to the credit card processing agent and the merchant need not be trusted with this sensitive information. XML encryption would conceal the credit-card number within the order entry document and only the credit card company would have the proper keys to decrypt the sensitive information. Encryption technology is complemented by data verification techniques to assure that message has not been modified as it travels over communication lines.

**XML Digital Signatures: Authentication**

A digital signature is a way to ensure that an electronic document is authentic: that you know who created the document and you know that it has not been altered in any way since that person created it. Digital signatures rely on certain types of encryption to ensure authentication. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures. Digital Signatures are a core piece of functionality required for a comprehensive XML Security architecture. Digital Signatures also provide integrity, as the signature will not verify if the content that the originator signed has been modified.

**XML Authorization: Access Control**

Authorization policies offer dynamic protection granularities ranging from a set of documents to specific elements within a document. Authorization policies are based on user credentials and on authorization rules at different granularity levels with different delivery options. For example: “Only programmers that are permanent staff can access documents related to the internals of the system” or “A class of documents can be accessed only by users that are more than 18 years old”.

**XML Validation: Well-Formed Data**

There are two kinds of documents that are associated with an XML instance: valid and well-formed documents. A well-formed document follows the grammar rules of XML and this is the minimum requirement for a document to be handled by an XML-enabled application. A valid document is a document conforming to a given template or schema. A well-regulated XML Security policy includes rules requiring a document entering or leaving the enterprise under go a conformance test that will determine whether that document instance matches a specific schema. This avoids the transmission or processing of corrupt data that might otherwise be a virus intended to disrupt a critical business process. Examples of industry-specific vocabularies: FPML, cXML, xCBL, RosettaNet messages and OAG BOD’s.

### **Next Generation XML Security Infrastructure**

The above requirements emphasize the need for an XML-based “information security firewall” that provides targeted *controlled access and exchange of XML content* as it passes within and out of enterprise networks. As opposed to the traditional notion of a “firewall” that operates as a filter restricting or allowing data to pass through but providing no security an XML-based information security firewall offers:

1. Policy based guidelines that extend enterprise security practices onto business data.
2. Data protection in networks as well as data stored on computers (i.e. transport as well as message security).
3. Fine-grained “element-level” XML security guaranteeing content-level confidentiality, data integrity, authentication and authorization.

## Forum Systems Solutions – Sign, Seal and Deliver

**Forum Systems Inc. develops and markets network security equipment that actively guards business-critical data as it moves between and within enterprises by protecting specific content within XML and non-XML documents – at the origin, during transmission and after it reaches its destination.**

The Forum Systems XML Security Appliance (Forum Systems Appliance) is the first true content-level security product designed specifically for secure business-to-business data movement in a cost effective hardware Appliance. It features content-level document security protection, in-line packet transparency performance, advanced auditing, dual-port flexibility and patent-pending ForumOS™ software.

The Forum Systems Appliance meets the demands for comprehensive Internet security that is specifically designed for the exchange of electronic business data with the following key features:

- Content-level confidentiality and integrity by selectively encrypting and decrypting sensitive data in-transit as well as in-storage.
- Sender authenticity using flexible, multi-part digital signatures within a single document.
- Rich security policy rules for greater control over data protection between the enterprise and business partners.
- High performance in-line processing providing transparent and seamless network connectivity.

Using Forum Systems XML security infrastructure Global 1000 companies, service providers, ISVs, and systems, integrators can build secure trading networks and web services for strategic applications such as: supplier procurement, financial exchanges and insurance processing.

# Forum Systems Appliance Subsystems

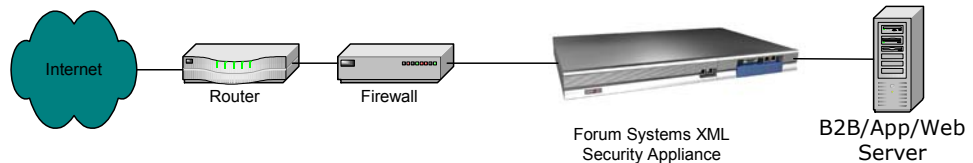
## Appliance ForumOS™

The most significant differentiator of Forum Systems XML Security solutions lies in the unique hardware implementation. The fact that there is no need to install or maintain any software components offers a level of reliability that is unmatched in pure-software implementations. Only the most relevant security features have been offloaded onto the Appliance leaving high-end software based security management infrastructures (Entrust™, RSA™, Baltimore™ et. al.) to handle enterprise wide security. Forum Systems Appliances focus on securing the front-line as data moves within and between the enterprises.

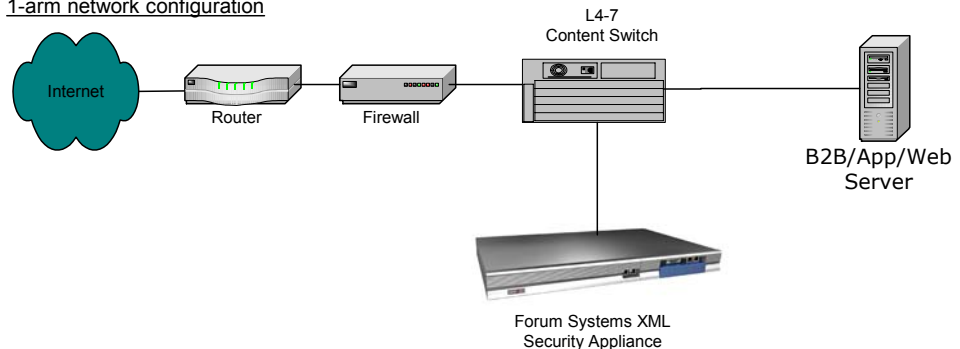
Forum Systems Appliances rely upon an on-board operating system called the ForumOS™ with the following benefits:

- Patent-pending extensible Java-based implementation for rapid system software upgrades.
- Allows dynamic upgrades to functionality using Pluggable Software Components architecture. Simply said, a developer can add new application services on the fly.
- Enhanced security that defends against application and network device attacks.
- Installs as an In-Line network device for plug and play, non-intrusive operation with easy integration into existing environments. In 1-arm configuration the Appliance works with standard content level routers for deep load balancing (see figure below)

### in-line network configuration



### 1-arm network configuration



The ForumOS™ is the core server behind the key subsystems described in the following sections of the White Paper.

## **Process Manager**

The Process Manager is the XML processing engine governing how in-bound and out-bound data is handled according to pre-defined policies. Data can be validated, transformed, secured, aggregated and then priority routed to the back-end server. Developers and system administrator can easily customize the Process Manager using the Forum XMLSec™ Developer workbench.

The key components of the Process Manager are Namespace, Document Identification Engine and Tasks and Task Lists, and are outlined below.

## **Namespace**

The Appliance organizes all properties, objects and services associated with in-coming and out-going data within a framework called a Namespace. The Namespace is used as a design time and run-time workspace where the required tools to perform data processing are loaded and manipulated.

There are number of system objects used to configure the Process Manager including:

- **Project Nodes:** A Project is used to classify, group and store a specific document-processing scenario. For example a company may map a project to general business process such as order entry or a vendor specific MRO procurement workflow. In each business scenario the *document processing tasks* are placed under the Project directory structure.
- **Folder and Sub-Folder Nodes:** A Folder and Sub Folder are used to classify, group and store the *document processing tasks* that apply to a specific Project. Folder Nodes are used for organizational purposes as well as version control capabilities.
- **Document Nodes:** A Document represents a structured data set that is being moved between two businesses. A Document can be a Purchase Order, Invoice or Bill of Lading. A Document is created from templates based off of sample XML, W3C schemas or DTD's. A unique document identity is assigned based upon any number of document criteria. For example, a "PriorityPO" document could be created that represents a conformant xCBL PO with a trading Partner of Dell and a \$ amount over 100,000. This document identity is used to route in-coming documents for data processing such as digital signatures, validation and transformation.
- **Process Nodes:** A Process contains the set of tasks that are used to manipulate a document before sending it onto its next destination.

## **Document Identification Engine**

The Document Identification Engine provides the capability to partially parse inbound documents and determine the proper routing sequence for the document. When a document is received that meets specific pre-set criteria, it will be forwarded to the appropriate document handler for processing. In order for the Appliance to process any incoming document the Appliance will need to detect the following:

1. The type of document including its content makeup (text, binary) and structure (XML, comma delimited).
2. The document identification to route the document to the specific data processing tasks.

## Tasks & Task Lists

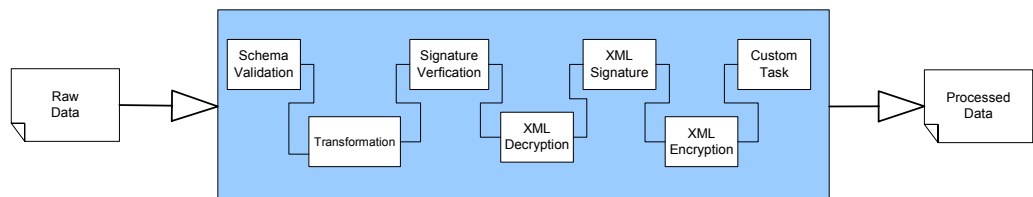
Forum Systems Tasks are the actions that can be executed on a document including:

- Digital Signature and Verification
- Validation
- Transformation
- Encryption and Decryption

A Task List is a series of these functions grouped together according to business policy. For example:

- The document is sent as an input parameter to a validation task
- The results are evaluated, if positive
- Sent to transformation engine process
- Signed by multiple, different signatures on a variety of document elements
- Sent to log manager
- Sent to backend server using an SSL connection

Using configurable Task Lists the Forum Systems Appliance allows companies to develop and dynamically enable customized data processing scenarios:



## **Security Manager**

The modular architecture of Forum Systems software diversifies functionality in an organized manner. At the heart of the product functionality are the security capabilities of the system. These security capabilities span device functionality, management and overall system design. The Security Manager is responsible for providing these security services to the system.

The features provided by the Security Manager include:

- XML Encryption and Decryption - Granularity of encryption is applied to the element (including start/end tags) or element content (between the start/end tags) as well as super encryption of the entire document. Encryption functionality provides the methods used to encrypt and decrypt XML content, as specified through the developer GUI. The Appliance conforms with the W3C XML Encryption specification by implementing the following methods:
  - Encryption of Elements
  - Encryption of Content
  - Decryption of Elements
  - Decryption of Content
- XML Digital Signatures: Complimentary and independent of XML Encryption, XML Digital Signatures are a core piece of functionality provided by Forum Systems. During business transactions, it is useful and often required for the authenticity of a request to be verified. A verifiable audit trail is also necessary in some environments. The use of digital signatures allows a transaction to be verified at multiple levels, and a history of the transaction sequence is easily ascertained. The Appliance provides signing capabilities in accordance to the W3C XML Digital Signature specification and implements the following signing types:
  - Enveloping Signatures
  - Enveloped Signatures
  - Detached Signatures
- Key Access and Storage – Interfacing capabilities to enterprise PKI software
- Access Control – To be provided is the ability to specify policies for accessing data over the Internet using an access matrix with authorization rules to control the disclosure of documents or portions of documents.

### **Communications Manager**

The protocol used to send messages is a key variable in network communications. For example there may be trading partners that can only send business documents using File Transfer Protocol and another might only be able to send their Purchase Order using standard E-Mail.

A key feature of the Appliance is to abstract the transport protocol used to communicate business data, such as:

- HTTP and HTTPS
- FTP
- SMTP

The Forum Systems Appliance provides web based configuration tools for managing protocol listeners including HTTP and HTTPS.

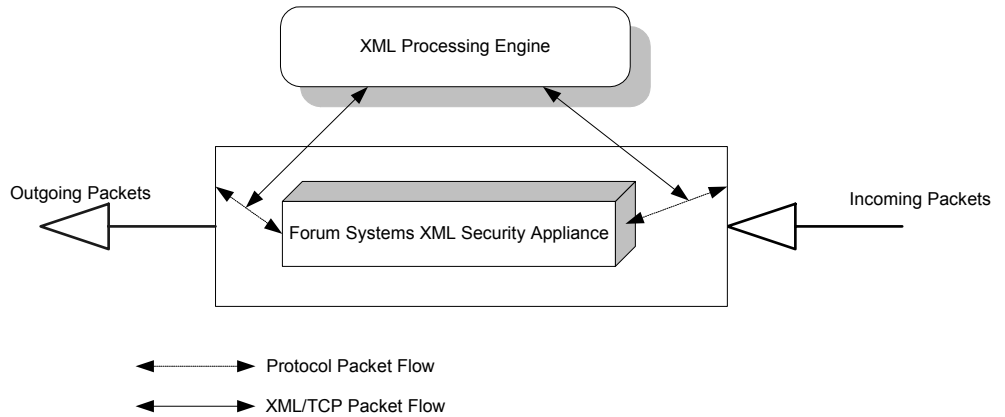
Documents coming inbound and outbound will be carried on top of these transport protocol in any number of message formats (encodings). The Appliance will be configured to handle a number of popular message formats, freeing the developer from having to manage marshalling and un-marshalling of data.

The Forum Systems Appliance will be able to support the following formats:

- XML/RPC
- Text/XML
- XML/SOAP

### **Network Manager**

The ForumOS™ implements a patent-pending architecture that provides a transparent mode of TCP packet forwarding between two Ethernet interfaces. The Network Manager intercepts incoming TCP streams, identifies them for XML processing, and then receives the result back for outbound transmission.



The key features of the Forum Virtual Driver are:

#### **Packet Capturing and Transmission**

Incoming TCP streams to the backend servers are intercepted based on configurable policies. The virtual driver identifies the packets destined for detected backend servers and forwards them to the XML processing engine (Process Manager). Streams that return from the XML processing engine are directly sent to the designed port.

#### **Protocol Control Packet Handling**

The Forum Appliance does not only deal with routing IP data packets. All other IP protocol packets such as ARP, RIP, IGMP and ICMP are directly sent to the outbound interface without any modification.

### **Log Manager**

Transaction visibility and traceability are a critical part of cross enterprise data exchange. Companies constantly anticipate a call from a customer that sounds like: “Our system sent you a PO a week ago for X, did you receive it?” This should be a very simple question to answer, but many integration systems will deliver information to the target system without keeping any history of what was delivered.

By placing the Forum Systems Appliance between the trading partner server and the enterprise application (E.g. ERP or SCM) every document that moves between the two systems can be identified and logged into persistent storage.

The Appliance allows archiving as whole or partial documents. Individual document elements maybe captured and logged with a timestamp or custom-tracking attribute for further auditing. This content-level logging allows companies to have tight data oversight and deep visibility into transactions. The Appliance offers an intuitive graphical interface to select which fields within the document to log.

### **Forum XMLSec™ Administrator**

The Forum XMLSec™ Administrator is a web based management and administration console. It is an easy to use application for monitoring as well as configuring all aspects of the Appliance including: server, security and network policies (see diagrams below).

Other benefits of the Administrator include:

#### **Monitoring**

The Appliance provides detailed information on resources and server load. This information is available through the web-based administration GUI. The underlying data is available to network and application management products like HP-OpenView, CA-Unicenter, Tivoli and BMC Patrol(Via SNMP as well as a JMX implementation which gives support for more sophisticated (application level) management protocols such as ARM2.)

#### **Transaction Visibility**

All logs are available through the web-based administration GUI as searchable XML files. The Appliance has an embedded ANSI 92 SQL database to assist with testing and pre-deployment activities.

#### **Component Management**

Component management, such as starting and stopping listeners are accessible via the web-based admin GUI.

The following figures illustrate the spectrum of features accessible via the web-based admin GUI:

### System Resources

**GENERAL**  
Forum Systems Serial Number: 0020021112 License: Unlimited Firmware version: 1.0  
Server Start Date/Time: Sun, 23 Dec 2001 02:24:20 PM PST  
Server Up-Time: 0 years, 0 months, 0 days, 0 h, 0 min, 31 s, 916ms

**MEMORY**

TOTAL	2969800	100%
FREE	1164960	39%
USED	1804640	61%

Server Policy	#Req	Max #Req	#Conn	Max #Conn	#Req/Conn
ADMIN					

LOGOUT STATUS: ONLINE FORUM SYSTEMS

### SSL Polices

**COMMUNICATION SECURITY**

**SSL POLICY**

SSL Policy Name:

Server Certificate:

Server Private Key:

**CERTIFICATE**

Belongs to: Alice  
Issued by: Alice  
Serial Number: 3B:F9:2D:A1  
Validity: Mon Nov 19 08:04:49 PST 2001 to Sun Feb 17 08:04:49 PST 2002  
Fingerprints: MD5: BB62 465F 2240 7621 93F7 640D 915F 89E0  
SHA: BF4E 8AF4 6FDE 3639 557D 7D33 4D60 FD02 2E07 7057  
Details: [Details](#)

**SSL CONFIGURATION**

Enable SSL v2  Enable SSL v3 Encryption Strength - High

**CLIENT-SIDE AUTHENTICATION**

Required  
 Optional  
 None

LOGOUT ACCEPT STATUS: ONLINE FORUM SYSTEMS

## Server and Network Policies

ABOUT HELP

GENERAL  
NETWORK  
SERVER  
KEY MGMT.  
SECURITY  
XML SECURITY  
ARCHIVING  
LOGS

SERVER POLICY

**Primary**

Policy Name:

Server IP:

Local Port:

Remote Port:

SSL Policy:

Enabled:  YES  NO

**Performance**

Minimum Number of Threads:

Maximum Number of Threads:

Maximum Idle Time (ms):

Maximum Read Time (ms):

**Miscellaneous**

Client Side Transparency:  ON  OFF

SNMP Traps:  ON  OFF

Proxy:  ON  OFF

LOGOUT

CREATE

STATUS: ONLINE

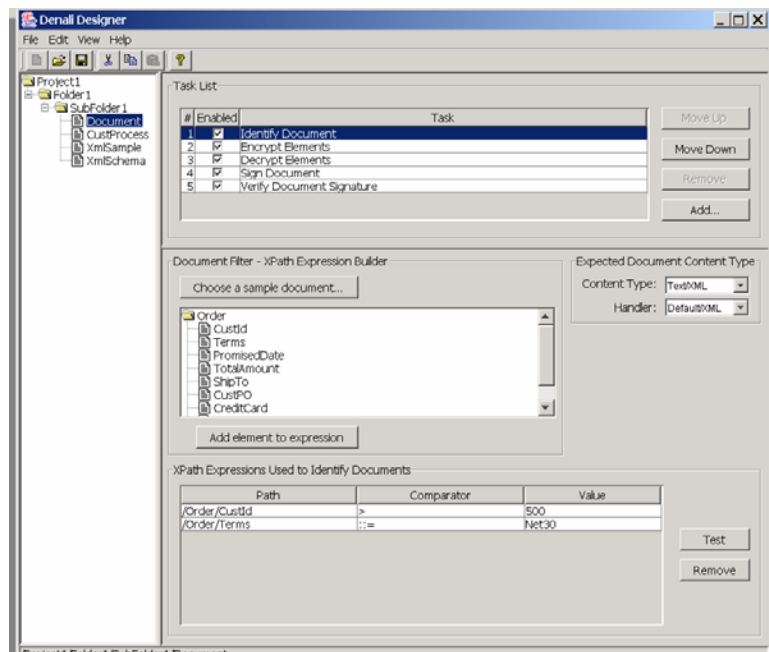
FORUM SYSTEMS

## Forum XMLSec™ Developer WorkBench

The Forum Systems Appliance offers an innovative package to deploy highly customized XML integration options. The Appliance comes with a world-class Java based development environment to develop personalized data processing tasks.

The easy to use, point and click GUI shields administrators from the prospect of supporting different XML grammars and setting up different processing rules for trading partners.

This screen shot offers a pre-view of the Forum XMLSec™ Developers Workbench:



The Forum XMLSec™ Developer WorkBench allows the administrator/developer to interact with the Appliance to specify the following data processing tasks:

<b>Document Identification</b>	Document identification tells the Appliance to route the document to a specific Default Process and in turn execute a series of functions on the document including encryption/decryption, verification, signing, transformation, validation and archiving. The rules that define document identify are based off of expressions applied to attributes and elements The identification expressions are created in this pane using XPATH expressions
<b>Document Encryption</b>	Document encryption applies a public key to an XML document's element or content or both in order to conceal the element or content or both those that were not intended to see them. By selectively encrypting the content of an XML document this document can be persistently protected until the decryption function is applied. This the primary method of data confidentiality provided by the Appliance.
<b>Document Decryption</b>	Document decryption applies a private key to an XML document's element or content or both in order to access previously encrypted elements or content or both.
<b>Document Signature Verification</b>	A digital signature that has been applied to an element or content or both element and will be verified by the recipient using the public key of the sender. This is signature verification process.
<b>Document Schema Validation</b>	Documents can be matched against a document template in order to verify the structure of this document. The template can be either a DTD or a W3Schema or an XML sample.
<b>Document Digital Signature</b>	In the digital world enterprises need digital signatures to perform sender authentication and data non-repudiation. A digital signature guarantees without doubt that the sender is indeed who he says he is and that they sent that particular message. A digital signature will vary with each transaction. The way to generate a digital signature that binds itself to a message as unique sender it to use public key cryptography. The algorithm guarantees that if a person encrypts a message with their private key, which they and they alone only hold that this message can be decrypted using the public key.
<b>Document Transformation</b>	Document transformation applies a template to an incoming XML document in order to change the structure or content of this document according to a set of business rules. These business rules will specifically described in XSLT compliant style-sheets.
<b>Archive and Logging Document</b>	Document archiving captures pre-determined elements and content into a persistent database for further analysis and auditing. The set of statements to select document data are created in the Workbench
<b>Data Processing Sequence</b>	The order of the tasks to be executed after document identification can be set at design time and manipulated at runtime.
<b>Dynamic Task Provisioning</b>	Personalized custom tasks maybe added at run-time using the Forum Systems Pluggable Software Components.