



A FORUM SYSTEMS TECHNICAL WHITE PAPER

## Web Services Security Management and Acceleration

---

Forum Systems Inc.  
95 Sawyer Road • Suite 110  
Waltham, MA 02453  
Phone 781-788-4213 • Fax 781-788-4201

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

## TABLE OF CONTENTS

<b>INTRODUCTION</b> .....	<b>2</b>
<b>Web Services</b> .....	<b>3</b>
<b>Data-Level Protection</b> .....	<b>4</b>
<b>STANDARDS-BASED WEB SERVICES SECURITY</b> .....	<b>5</b>
<b>WS-Security</b> .....	<b>5</b>
<b>XML Encryption</b> .....	<b>5</b>
<b>XML Digital Signatures</b> .....	<b>5</b>
<b>Security Assertion Markup Language</b> .....	<b>5</b>
<b>Emerging Standards</b> .....	<b>5</b>
<b>MANAGING AND ACCELERATING WEB SERVICES SECURITY</b> .....	<b>6</b>
<b>FORUM SYSTEMS PRODUCTS</b> .....	<b>7</b>
<b>Document Identification</b> .....	<b>8</b>
<b>Authentication and Access Control</b> .....	<b>8</b>
<b>Content Processing</b> .....	<b>9</b>
<b>Communications Management</b> .....	<b>10</b>
<b>Web Services Monitoring</b> .....	<b>10</b>
<b>Hardware Security Module</b> .....	<b>10</b>
<b>Management and Administration</b> .....	<b>11</b>
<b>HARDWARE-BASED WEB SERVICES SECURITY</b> .....	<b>13</b>

## Introduction

**This document is a technical primer for the Forum Systems product line. For specific product features, please consult the appropriate product datasheet at [www.forumsys.com](http://www.forumsys.com).**

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?

## Web Services

In the extended enterprise, the boundaries of business partners are blurred with closer coordination of design, development and marketing activities giving way to stable collaborative relationships. And Web Services are the driving engine behind the extended enterprise using open standards to implement dynamic, streamlined and collaborative electronic business processes that create new revenue opportunities and increased operational efficiencies.

The foundation building blocks for Web Services are:

- **XML** as the Lingua-Franca of business data representation. Using XML, it is possible to create self-describing business documents that contain active and context sensitive information that can be readily processed by machines, applications and humans. <http://www.w3.org/XML/>
- **SOAP** defines the format of a message that is to be exchanged by two parties with any number of intermediaries. SOAP allows the construction of remote procedures and networked application services that are known as Web Services. The SOAP Envelope, Header(s) and Body constructs are well-defined in structure; however, their content can change throughout a SOAP documents lifecycle. <http://www.w3.org/TR/soap12-part1/>
- **XML Schema** provides the mechanism for describing XML message formats and the constraints on the contained text. XML Schema allows companies to standardize their data models on industry-specific schemas that define the structure and business rules of the data they exchange with business partners. <http://www.w3.org/XML/Schema>
- **Web Services Description Language (WSDL)** is an XML-based document format that provides the “recipe” for Web Services usage. WSDL files contain both interface and implementation for functionality, and leverages SOAP and XML Schema for well defined message content. <http://www.w3.org/TR/wsd/>
- **UDDI Directory** (Universal Description, Discovery and Integration) allows users (machines or humans) to locate relevant Web Services over a distributed network. [http://uddi.org/pubs/uddi\\_v3.htm](http://uddi.org/pubs/uddi_v3.htm)

Along with the benefits of Web Services comes a new set of information security challenges :

- Unauthorized information disclosure during collaborative activities .
- Exposure of sensitive application interfaces via internal and external Web Services .
- Compliance to government regulatory initiatives such as Federal E-SIGN law, eGov Strategies, Health Insurance Portability and Accountability Act and Gramm-Leach-Bliley.
- Inadequate protection of data on desktops, application servers and mobile devices .
- XML-related threats against Web Services ranging from exploits, breaches to outright attacks .

## Data-Level Protection

Unfortunately, today information security is a technical afterthought too dependant on network-level security. The most common response to Web Services security is turning on Secure Sockets Layer (SSL) or using a VPN. However, this only provides in-transit data confidentiality (and limited point-to-point authentication) between two respectively-enabled parties. Network-level security lacks the necessary "data-level" intelligence required to *persistently* protect data at every step of a complex business process.

Data-level security addresses the following Web Services security requirements:

- **Message Exchange Privacy** — SOAP/XML is human readable plain text that explicitly describes information it carries, leaving Web Service requests and responses vulnerable to theft and misuse. Message exchange privacy assures messages are not visible to anyone except the two parties involved. Transport encryption provided by Secure Sockets Layer (SSL) or VPNs (Virtual Private Networks) does not prevent unwanted information disclosure as data travels from one intermediary to the next.
- **Payload Integrity** — Due to the store and forward architecture of Web Services, the integrity of data at rest, in storage or in processing is of primary concern. Payload integrity checking should be a persistent function (not transport-centric) that provides assurances against tampering and forgery across time and space. Using digital fingerprints that are bound to each message, recipients can verify that data is in its original form prior to consuming it.
- **Identity Authentication** — In the world of Web Services, authentication is the process of making sure that the entity (person or machine) requesting the Web Service is really who they claim to be. Authentication requires evidence, known as credentials. A user could present a password as its credentials and if these credentials can be verified as a valid digital identify, then it is assumed the user is who s/he claims to be. In a Web Services world, identity authentication functions seamlessly in a distributed or federated trust model where de-centralized authorities vouch for a user's identity.
- **Data Authorization** — Once a user's identity is authenticated, access is determined by checking information about the user against some access control information present in what is typically called an Access Control List (ACL). Data bound authorization schemes using SAML add portability and interoperability to user credentials, authentication information and access control privileges. A Web Service can simultaneously consume a transaction as well as make authorization policy decisions with out the need for proprietary interfaces.

## Standards-Based Web Services Security

The Web Services security specifications available from the W3C, IETF and OASIS provide a robust framework for implementing fine grained Data-Level Security policies for XML Web Services. These specifications describe rich methods to protect data - in-motion, in-processing, as well as in-storage.

### WS-Security

WS-Security is a set of tightly related specifications that describe SOAP-specific mechanics for message protection including message integrity, message confidentiality and message authentication. WS-Security is designed to work with a variety of existing security models including PKI (Public Key infrastructure), Kerberos, and SSL since it supports multiple security tokens, multiple trust domains, multiple signature formats, and multiple encryption technologies. <http://www-106.ibm.com/developerworks/library/ws-secure/>

### XML Encryption

Since 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 see specific data. Using XML Encryption, targeted information inside a document may be concealed and only available to authorized parties. XML Encryption would be used to selectively conceal information such as credit card numbers or shipping addresses within Web Service requests and responses. <http://www.w3.org/TR/xmlenc-core/>

### XML Digital Signatures

A Digital Signature is the electronic equivalent of an individual's pen-and-ink signature. An XML Digital Signature is attached to a specific document instance allowing the recipient to verify the identity of the document owner/creator – not just the server that transmitted the document. XML Digital Signatures also provide a permanent method of document integrity checking where any part of a document can be verified for tampering or corruption regardless of time and space. <http://www.w3.org/TR/xmldsig-core/>

### Security Assertion Markup Language

SAML provides Single Sign-on and distributed authentication capabilities in a federated trust model. Users can be authenticated between multiple security domains because SAML assertions travel with a document. A SAML Authentication Assertion is a statement that asserts that the user has been authenticated by the sender/creator of the assertion. SAML Attribute assertions contain specific information about the user. A SAML Authorization assertion identifies what the user is authorized to do. <http://xml.coverpages.org/draft-sstc-ff3-saml-spec-00.pdf>

### Emerging Standards

**WS-Policy:** describes the capabilities and constraints of the security (and other business) policies on intermediaries and endpoints (e.g. required security tokens, supported encryption algorithms, privacy rules).

**WS-Trust:** describes a framework for trust models that enables Web services to interoperate securely.

**WS-Privacy:** describes a model for how Web services and requesters state privacy preferences and organizational privacy practice statements.

**WS-SecureConversation:** describes how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys.

**WS-Federation:** describes how to manage and broker the trust relationships in a heterogeneous federated environment, including support for federated identities.

**WS-Authorization:** describes how to manage authorization data and authorization policies.

**XACML:** (Extensible Access Control Markup Language) describes how to express access control policies within a Web Service.

## Managing and Accelerating Web Services Security

Forum Systems Inc. develops and markets award-winning Web Services security infrastructure that actively guards data as it moves between and within enterprises by protecting specific content within XML and non-XML documents throughout the content lifecycle – at the origin, during transmission, and after it reaches its destination.

Forum Systems solutions offer the following unique differentiators:

**Accelerated Content Security** — Forum Systems solutions are designed to overcome performance demands of real-time XML Web Services security by enabling fast-path processing of the new “ContentLayer” within today’s Web Services business exchanges. Forum Systems hardware-assisted products include patent-pending dynamic content security processing capabilities that are dedicated to the pursuit of high performance XML Web Services.

**Web Services Security Management** — Web Services Security Management allows security designers and administrators to make sense of Web Services security specifications and gain control of policy variability, such as automating trading partner key maintenance and the configuration of granular, content-filtering rules. Forum Systems Enterprise Class design-time and run-time tools pass the grade on functional, operational and management criteria for Global 1000 companies.

Using Forum Systems Web Services security infrastructure, Global 1000 companies, government agencies 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 Products

The Forum Systems product line includes:



**Sentry™** — Sentry™ is a comprehensive Web Services Security Management and Acceleration solution that functions as a trusted intermediary for exchanging XML messages between an enterprise and its business partners.

**Presidio™** — Presidio™ is the only Appliance-based solution that provides secure data messaging using both PGP Encryption as well as XML Web Services security. Using Presidio™, an enterprise can use the same platform to migrate towards secure SOAP/XML data while protecting legacy data.

**XWall™** — XWall™ is the only solution that is specifically designed to detect and prevent XML-related threats and attacks from the "network edge to the application". Using XWall™, enterprises can intelligently detect and prevent abuse and misuse of Web Services by both trusted and un-trusted users.

The following sections describe functionality within the Forum Systems product line.

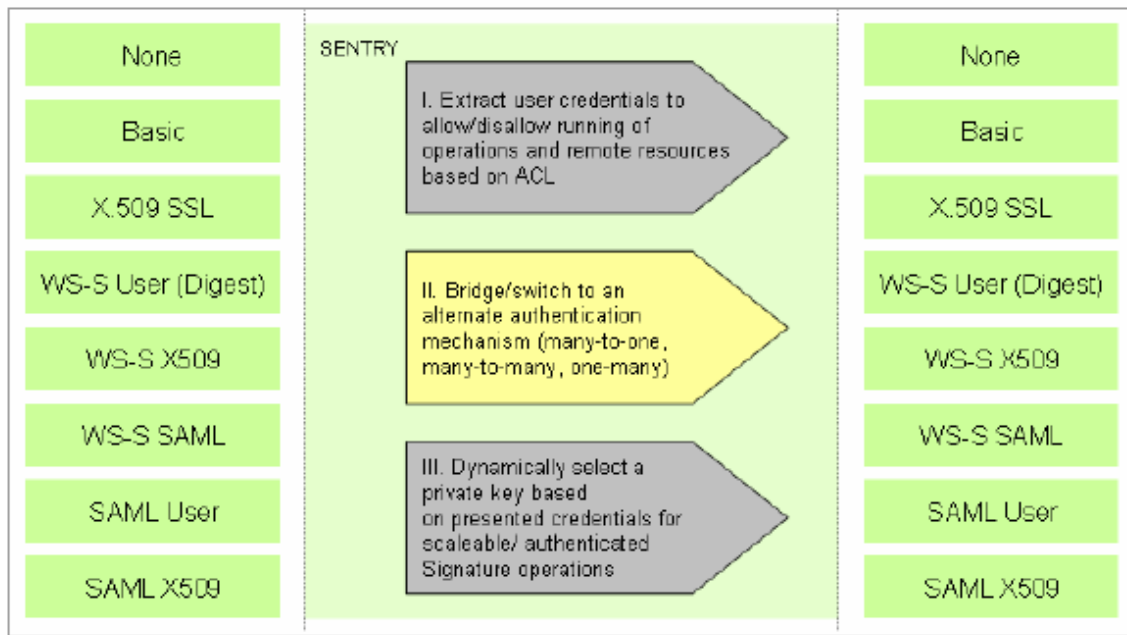
### Document Identification

Document Identification provides the capability to partially parse inbound documents and determine the proper routing sequence for the document. When a document is received that meets a specific pre-set criteria, it will be forwarded to the appropriate Content Processing Tasks (see Content Processing section below).

### Authentication and Access Control

Forum Systems Authentication and Access Control uniquely support both transport-centric as well as document-centric mechanisms. Transport-centric authentication includes HTTP Basic Authentication and SSL Client Certificates. Document-centric authentication includes SAML and WS-Security Headers.

The following diagram illustrates three use cases of Forum Authentication and Access Control:



## Content Processing

Forum Systems offers optimized Content Processing functions that can be dynamically configured to target transaction request and/or response payloads. Built-in Content Processing Tasks include:

- SOAP/XML Digital Signatures
- SOAP/XML Encryption and Decryption
- PGP Encryption and Decryption
- PGP Digital Signatures
- SOAP/XML Schema Validation
- SOAP/XML Intrusion Detection and Prevention
- SOAP/XML Transformation
- WS-Security Authentication and Access Control
- SOAP/XML Archiving
- Content Based Routing

## Communications Management

A key variable in Web Services exchanges is the application transport protocol on top of which messages are delivered. For example, there may be a trading partner that can only send business documents using File Transfer Protocol (FTP) and another might only be able to send their Purchase Orders using standard E-Mail.

A key feature of Forum products is an abstract application transport protocol framework that supports:

- HTTP and HTTPS
- FTP
- SMTP
- JMS

## Web Services Monitoring

Business intelligence starts with logging every business transaction entering and leaving the enterprise. In fact, deep transaction visibility and traceability are critical in complying with corporate and government information security mandates. Enterprises should anticipate answering customer questions such as: “Our system sent you a PO ten minutes ago for X. Did you receive it?”

Forum Systems Web Services Monitoring transparently tracks the activities of Web Services as well as assesses the reliability and downtime of Web Services. Web Services Monitoring includes taking partial or complete snapshots of transactions accompanied by a timestamp for further auditing or proof of non-repudiation.

## Hardware Security Module

Private keys are central to cryptographic operations used in Secure Sockets Layer (SSL) and Web Services Security. They are the crown jewels of an organization and their security *must be* guaranteed against any sort of compromise. Software-based cryptographic toolkits, by their very portable nature, cannot completely protect against private key theft and attack such as key copying and modification— which can readily result in significant financial loss and business disruption. Imagine the value of a digital signature on a transaction where duplicate private keys exist— there will be no way to assure the authenticity of the transaction. The entire viability of cryptographically-protected transactions relies on the integrity of private keys.

The Forum HSM™ (Hardware Security Module) ensures the highest level of protection for Web Services by offering an integrated security solution that stores private keys in a tamper-resistant, hardware security module that is impervious to attack. The HSM also complies with the Federal Information Processing Standard (FIPS) 140-2 Level II specification for private key life cycle management (key generation, importation, backup and recovery) as well as secure execution of cryptographic algorithms – an essential requirement for public key-enabled U.S. and European e-Government applications.

## Management and Administration

Forum Systems products are designed for ease of use and usability by offering the right tools for the right purpose—reducing complexity and operations costs. The following table describes Forum Systems enterprise class administrative and management user interfaces:

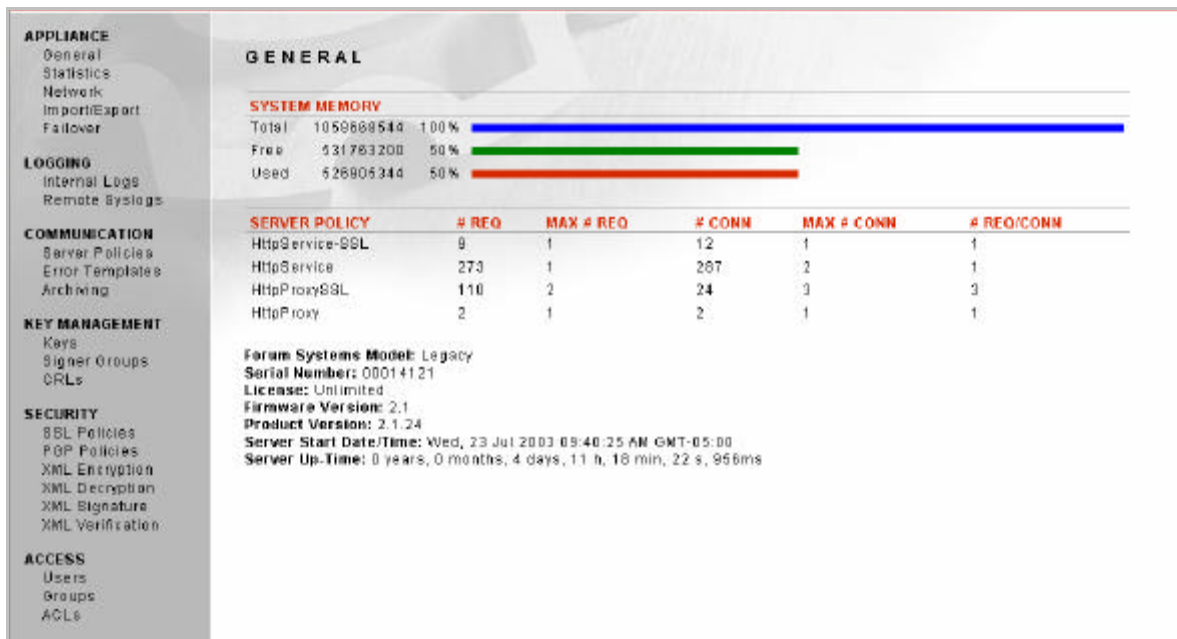
TOOL	METHOD OF COMMUNICATION	USER ROLE
Command Line Interface	CLI can be accessed via several methods. You may access the serial console, which can be used with terminal emulation software. Once the Appliance has been configured, you may also access the CLI via SSH.	IT Administrators or Network Administrators
Workbench	Workbench communicates using SOAP / HTTP.	Security Managers
WebAdmin	WebAdmin communicates using HTML / HTTPS.	System Administrators

The Forum WebAdmin™ tool allows network and system administrators to:

- Manage your network configuration settings.
- Import /Export configuration files.
- Manage Failover and Failback Policies.
- Manage a variety of system logs in six categories including SysLog and SNMP settings.
- Configure Server Policies that deploy HTTP, HTTP(S) and FTP communication managers.
- Configure policies that allow for bulk encryption and bulk decryption with PGP over FTP.
- Manage Key Pairs and Public Certificates for PKCS as well as PGP Keys.
- Manage CRLs and CA integration such as OCSP and CSR policies.
- Manage XML Encryption and Decryption Policies.
- Manage XML Signature and XML Digital Signature Verification Policies.
- Manage users, groups and access control lists .

(This is a partial feature list; please see specific product data sheets for current features , available at [www.forumsys.com](http://www.forumsys.com).)

This diagram illustrates the graphical user interface of the Forum XMLSec™ WebAdmin:

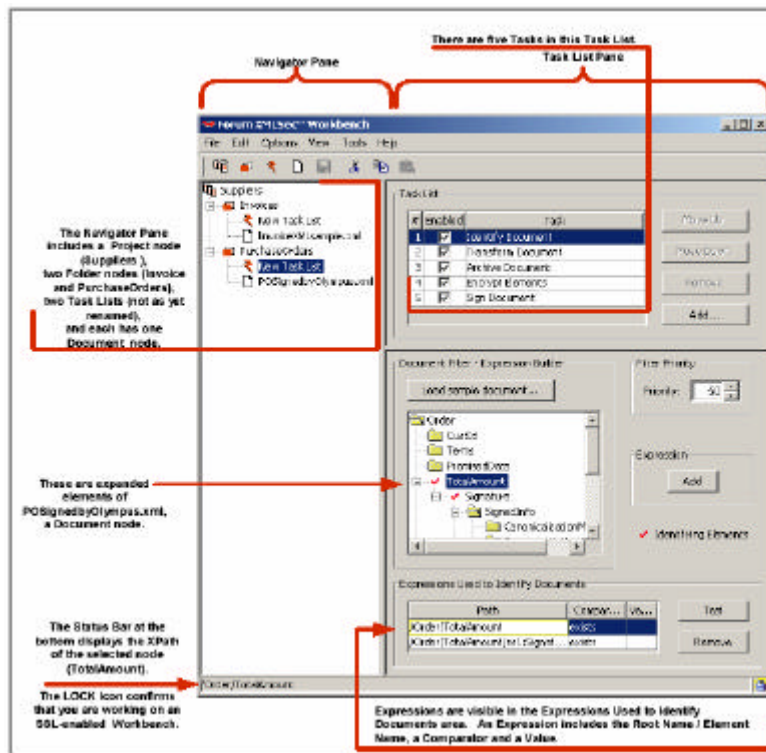


The Forum XMLSec™ Workbench is a visual development environment used by Security Managers to:

- Manage XML security Projects and Task Lists.
- Set filter priorities and create XPath expressions to uniquely identify Task list.
- Monitor design-time processes at any processing step by running the Task list.
- Configure XML encryption at the element or content level.
- Configure XML decryption at the element or content level.
- Configure XML signatures on the entire document.
- Configure SOAP/XML Intrusion Detection and Prevention rules .
- Configure XML digital signature Verification tasks .
- Configure corporate/customer requirements using XSLT Style sheets.
- Configure individual elements, entire documents and/or both to store to an Oracle, MySQL or DB2 database during Archive Document task.
- Map credentials from Protocol to document-centric (SSL to SAML).
- Configure dynamic credential binding of private keys for signing.
- Configure Access Control options based on transport, protocol or document

(This is a partial featurelist; please see specific product data sheets for current features available at [www.forumsys.com](http://www.forumsys.com).)

This diagram illustrates the graphical user interface of the Forum XMLSec™ Workbench:



Forum Global Device Management simplifies the management of multiple Forum Servers including:

- Replicating the configuration of one machine minus network information.
- Allowing granularity of configuration.
- Automating the process of importing and exporting configurations .

## Hardware-Based Web Services Security

The Forum Systems product line is delivered on an Appliance form factor that can best handle the resource and performance demands of XML Web Services security operations such as XML Digital Signatures and XML Encryption. Hardware-Based solutions such as the Sentry™ 1500 Series, also offer the following advantages over their software counterparts:

- **Hardened Security** — A private key is considered to be the ‘crown jewel’ of the company and protecting it should be a foremost priority. Hardware-Based solutions integrate a Hardware Security Modules (HSMs) to directly address the following security issues:
  - **Key-Finding** describes a threat by which an unauthorized user can locate the private key used in a cryptographic security scheme. Once the key is found, the unauthorized user can impersonate the legitimate user in electronic transactions.
  - **Buffer Overflows** are attributed to a majority of security attacks against networking servers and are one of the most devastating security exploits. Even the widely used OpenSSL security library suffered a buffer overflow exploit.
  - **Secure Cryptography** should not be taken for granted and HSM™ separates the critical security functionality from the application software. This allows the application developer to focus on improving the quality of the application, assured of the integrity of the security components.
- **Price / Performance** — As XML Web Services security transactions increase it will be important to maintain acceptable application response times. Incrementally adding general purpose processors to maintain response time thresholds with increasing transactions per second (TPS) requirements is not scalable and is exponentially cost prohibitive, especially for ‘large’ 2048-bit private key RSA operations. Even when response times may initially be acceptable with software-based solutions the Price/Performance advantages of Hardware-Based cryptographic chip sets over general purpose processors becomes self evident.
- **Manageability** — A Hardware-Based solution to XML Web Services security has a number of operational benefits including:
  1. **Application agnostic deployments.** As the number of trading partners and SOAP/XML message types increases, API-driven security toolkits become not only insecure but also a highly inefficient proposition. A Hardware-Based solution can be deployed in a central data center to service all Web Services – transparently to the application and user.
  2. **Centralized policy management:** Web Services security policies contain ultra-sensitive and mission-critical information. Strictly controlling the rules and parameters of these policies across multiple applications becomes a necessity. A centralized policy management system reduces operational costs and saves time by streamlining the entire Web Services Security Management life-cycle from design, configuration to deployment.