USING FORUM SENTRY TO IMPLEMENT
NI ST PUBLICATION 800-95
"GUIDE TO SECURE WEB SERVICES"
Legal Marks
No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.


All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2012 Forum Systems, Inc. – All Rights Reserved.

Using Forum Sentry to Implement NIST Publication 800-95 “Guide to Secure Web Services”

D-ASF-SE-030342
Table of Contents

INTRODUCTION ........................................................................................................................................... 4
   Sentry Technology Components Used........................................................................................................ 4
   Platforms................................................................................................................................................... 5
2. Background to Web Services and Their Relationship to Security...................................................... 6
   2.1.1 Web Services Discovery.................................................................................................................. 6
   2.1.2 Web Service Messaging................................................................................................................ 6
   2.1.3 Web Portals ..................................................................................................................................... 6
   2.1.4 Web Services Roles, Modes, and Properties.................................................................................. 6
   2.2 Elements of Security........................................................................................................................... 6
   2.3 Web Services Security........................................................................................................................ 7
   2.4 Meeting the requirements for Securing Web Services....................................................................... 7
   2.5 Core Services ..................................................................................................................................... 7
   2.6 Threats Facing Web Services ........................................................................................................... 8
   2.7 Common Risks Facing Web Services .............................................................................................. 11
   2.8 Web Services’ Interfaces with Network/Infrastructure Security Architectures.................................. 11
   2.9 Summary .......................................................................................................................................... 11
3. Tables of Standards ........................................................................................................................... 12
   3.1 Message Formats and Standards........................................................................................................ 12
   3.2 Protocol Formats and Standards......................................................................................................... 13
   3.3 Identity Formats and Standards......................................................................................................... 14
   3.4 Security Standards and Features....................................................................................................... 15
About Forum Systems................................................................................................................................ 16
INTRODUCTION

The National Institute of Standards and Technology (NIST) released publication 800-95 entitled “Guide to Secure Web Services” which provides context of the challenges and underlying technologies involved in securing XML, SOAP, and REST based services. This document is available online at the following link:


Forum Systems – a wholly owned subsidiary of Crosscheck Networks - is a leader in Service Oriented Architecture (SOA) and Portal security. Through comprehensive threat mitigation and trust enablement, the Forum Sentry Security gateway technology provides enterprises and organizations with the foundation for achieving secure service federation. Processing more than one billion transactions per day worldwide, the FIPS- and DoD-certified Forum Sentry XML Gateway offers the industry's most comprehensive protection against HTML, XML, SOAP and REST based vulnerabilities. Forum is a pioneer in XML security, and Forum Sentry has been issued an industry-first patent (7,516,333) providing broad coverage for XML Security functions such as XML-encryption, XML-decryption and XML-signatures as well as security acceleration on a network appliance. Forum Systems products provide simplified integration and task processing with over 100 built-in standards-based real-time processing tasks.

This document will specifically highlight how Forum Sentry provides the entire breadth of functionality to achieve all referenced aspects of NIST publication 800-95 and is the industry’s leading solution for NIST recommended security protection of deployed services.

Sentry Technology Components Used

The technology discussed in this document utilizes the following technology components that are available and integrated with the Forum Sentry product.

<table>
<thead>
<tr>
<th>Protocol Policies</th>
<th>HTTP, FTP, SFTP, SMTP, IBM MQ, Tibco EMS, WebLogic JMS, JBOSS, Active MQ, AMQP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Policies</td>
<td>WSDL, XML, REST, JSON, HTML</td>
</tr>
<tr>
<td>Mediation Policies</td>
<td>XSLT, Attribute Mapping, Content Mapping, RegEx</td>
</tr>
<tr>
<td>Identity Policies</td>
<td>LDAP, Active Directory, Siteminder, Tivoli, Oracle AM, OpenSSO, OpenAM, OAuth, REST, WS-Trust, XACML</td>
</tr>
<tr>
<td>Governance Policies</td>
<td>Authorization, Authentication, Flow Control, Size Control</td>
</tr>
</tbody>
</table>
**Platforms**

The use case can be implemented using any of the following available Forum Sentry form factors:

<table>
<thead>
<tr>
<th>FIPS 140-2 Hardware</th>
<th>GNU/Linux</th>
<th>Solaris</th>
<th>Windows XP</th>
<th>VM</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
2. **Background to Web Services and Their Relationship to Security**

NIST publication 800-95 introduces web services and variants of deployed technologies involved in web services. Section 2 portions of the NIST document are itemized below with Forum Sentry capabilities described as applicable for each.

### 2.1.1 Web Services Discovery

Forum Sentry provides UDDI retrieval of WSDL information, and also provides on-board secure repository storage of WSDL artifacts. WSDL definitions can be aggregated on Forum Sentry and exposed as virtual WSDL API services combining multiple services and services operations into single virtual WSDL definition files that have a single IP and Port and combined schema items from all selected operations. These WSDL services can be republished by Forum Sentry to the Web Services Discovery repository.

### 2.1.2 Web Service Messaging

Forum Sentry provides messaging support for XML, JSON, REST, and SOAP. SOAP support includes SOAP 1.1 and SOAP 1.2, with full support also provided for SwA MIME, DIME, and MTOM standards for binary formats of SOAP content delivery. Forum Sentry provides messaging format conversion among these messaging types through transformation, mapping, node manipulation, 3rd party message enrichment services, and standards-based conversions.

### 2.1.3 Web Portals

Forum Sentry provides messaging support for HTML and provides on-board WAF policy inspection rules that provide deep content inspection of HTML message variants in both the request and response pattern.

### 2.1.4 Web Services Roles, Modes, and Properties

Requester, Provider, and Intermediary web services are all client and/or server based targets that Forum Sentry provides gateway processing of message flows for invocations among service roles, as well as clients and providers of the services.

### 2.2 Elements of Security

Forum Sentry provides extensive underlying technology components to meet the security threat and vulnerability implications called out in this NIST section of the 800-95 publication. Specifically:

- **Identification and Authentication**: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

- **Authorization**: The permission to use a computer resource, granted, directly or indirectly, by an application or system owner.

- **Integrity**: The property that data has not been altered in an unauthorized manner while in storage, during processing, or in transit.

- **Non-repudiation**: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information.
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Privacy: Restricting access to subscriber or relying party information in accordance with Federal law and organization policy


2.3 Web Services Security
NIST publication states that web services security dimensions include Secure Messaging, Resource Protection, Contract Negotiation, and Trust Relationships. Forum Sentry technology meets all these aspects of security technology.

Forum Sentry provides for Secure Messaging via SSL/TLS over all supported protocols, including HTTPS. Forum Sentry has broad support for WS-Security 1.1 and WS-Security 2004 as well as comprehensive support for OASIS and W3C security standards around XML Encryption, XML Signature, WS-Encryption, and WS-Signatures.

Protection of resources is assured through the FIPS 140-2 secured Forum Sentry architecture. Forum Sentry has achieved a FIPS 140-2 Level II certification for the entire product perimeter. This assures that underlying policy artifacts, keying information, and the system integrity itself has been designed and implemented according to the most rigorous standards in the industry.

Contract Negotiation and Trust Relationships can be accomplished using Forum Sentry 2-way SSL with X.509 client authentication and document-based Signature Verification using Public/Private keys.

2.4 Meeting the requirements for Securing Web Services
NIST specifies the industry standards for Security Management, Identity Management, Message Security, Reliable Messaging, Policy, SOAP and XML Security, Access Control, and Transport Layer Security. Forum Sentry supports all standards highlighted by NIST as well as many others that are used in new technology formats for mobile computing security, cloud computing security, and ESB messaging security for JMS message patterns. Specifically, Forum Sentry provides simply rule policy creation and enforcement for the following standards based formats:


2.5 Core Services
The NIST documented core services all comprise the typical set of client and service portions of the business transactions that Sentry intercepts and provides deep-content inspection for security, identity, governance, and mediation. Management services, communication services, policy services, and
security services are noted, but also are extended to mobile services, identity services, data storage services, and cloud or virtual services. Since Forum Sentry provides comprehensive deep-content parsing support for the underlying messaging technology formats, all of these core services fall within the traffic patterns that Forum Sentry provides protection.

2.6 Threats Facing Web Services
NIST extracts the top threats facing web services from WS-I and list them as follows*:

- **Message alteration.** An attacker inserts, removes or modifies information within a message to deceive the receiver.
- **Loss of confidentiality.** Information within a message is disclosed to an unauthorized individual.
- **Falsified messages.** Fictitious messages that an attacker intends the receiver to believe are sent from a valid sender.
- **Man in the middle.** A third party sits between the sender and provider and forwards messages such that the two participants are unaware, allowing the attacker to view and modify all messages.
- **Principal spoofing.** An attacker constructs and sends a message with credentials such that it appears to be from a different, authorized principal.
- **Forged claims.** An attacker constructs a message with false credentials that appear valid to the receiver.
- **Replay of message.** An attacker resends a previously sent message.
- **Replay of message parts.** An attacker includes portions of one or more previously sent messages in a new message.
- **Denial of service.** An attacker causes the system to expend resources disproportionately such that valid requests cannot be met.

*More information about the threats and challenges facing Web services can be found in Security Challenges, Threats and Countermeasures at [http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf](http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf)

All technologies noted by NIST that protect against these threats are built-in features of Forum Sentry. To specifically highlight how Forum Sentry defends against these threats, the preceding list is repeated with the Forum Sentry technology that handles them.

- **Message alteration.** An attacker inserts, removes or modifies information within a message to deceive the receiver.
  - ✓ Forum Sentry™ provides schema validation which ensures that the structural integrity of
the message is maintained. Additionally, Integrity is ensured using the digital signature standards to sign and verify signatures on-board Forum Sentry to ensure integrity of the message is maintained and no alteration occurred.

**Loss of confidentiality.** Information within a message is disclosed to an unauthorized individual

- Forum Sentry™provides comprehensive support for data-level and protocol-level encryption. Additionally, hashing algorithms are provided along with RegEx pattern replacement. All of these features enable policy-based confidentiality assurance where sensitive information is protected throughout the lifecycle of the document.

**Falsified messages.** Fictitious messages that an attacker intends the receiver to believe are sent from a valid sender

- Forum Sentry™provides 2-way SSL strong authentication and replay detection for all message-based security formats to detect falsified clients that attempt to capture and replay messages to gain access.

**Man in the middle.** A third party sits between the sender and provider and forwards messages such that the two participants are unaware, allowing the attacker to view and modify all messages

- Forum Sentry™performs both SSL Termination and SSL Initiation. With both, a strong authentication X.509 path validation with revocation checking is performed. To prevent man-in-the-middle attached, Host verification is performed to ensure that the target of the SSL connection matches the issued DN of the X.509 certificate that the server is presenting for the SSL session. This X.509 is also authentication against the CA chain that issued is to ensure a valid certificate is being presented by this service.

**Principal spoofing.** An attacker constructs and sends a message with credentials such that it appears to be from a different, authorized principal

- Forum Sentry™enforces integrity checks for digital signature verification combined with designated targets for the signature digest locations. This prevents the attack of spoofing the principal or other aspects of a valid credentials by reconstructing the message and providing a valid signature in other locations of the message.

**Forged claims.** An attacker constructs a message with false credentials that appear valid to the receiver
Forum Sentry™ authenticates and authorizes the message with the credentials against a variety of industry identity infrastructures. Role information and correlations of tokens with sources can be checked and enforced by Sentry to detect forgery attempts.

**Replay of message.** An attacker resends a previously sent message

- Forum Sentry provides replay detection of security based standards such as WS-Security Identity Tokens and Signed Messages. Replay detection prevents a previously submitted message from being re-submitted without a unique wire signature that would be required by a dynamically generated security signature.

**Replay of message parts.** An attacker includes portions of one or more previously sent messages in a new message

- Forum Sentry™ enforces integrity checks for digital signature verification combined with designated targets for the signature digest locations. This prevents the attack of spoofing the principal or other aspects of a valid credentials by reconstructing the message and providing a valid signature in other locations of the message.

**Denial of service.** An attacker causes the system to expend resources disproportionately such that valid requests cannot be met.

- Forum Sentry™ provides rate-based and size-based governance enforcement for SLA rate enforcement, infrastructure protection, and denial of service detection and prevention. Forum Sentry IDP (Intrusion Detection and Prevention) rule architecture provides actions on rate triggers which include future access restrictions that apply once a trigger is detected and can throttle or block offending users for specified or indefinite (Administrator interacted) intervals.
2.7 Common Risks Facing Web Services
NIST details how traditional security technologies such as firewalls and WAFs are inadequate to secure web services. Perimeter based network security technologies such as IDS systems are also inadequate due to several factors, including transport protocols such as HTTP that this infrastructure allows to pass through, the complex nature of the actual message payloads require deep-content inspection. Forum Sentry™ is designed to handle and parse complex message formats at the TCP application 4-7 layers with deep-content inspection of HTML, XML, REST, JSON, SOAP, and SwA message patterns. This addresses the necessary complexity of providing risk mitigation to these message transmission formats by ensuring the data patterns are processed and inspected at the content-level on request and/or response patterns.

2.8 Web Services’ Interfaces with Network/Infrastructure Security Architectures
PKI is an essential aspect of the underlying technologies of XML Encryption, XML Signatures, SSL/TLS, and other security standards that are derived from these. NIST points out that the interfaces with other infrastructure and security architecture require adept PKI capabilities as well as standards based authentication and authorization features such as SAML and XACML. Forum Sentry provides a comprehensive centralized PKI Key management feature set, which includes key lifecycle management, and FIPS 140-2 Level II and Level III key storage security. Forum Sentry PKI engine has been certified by the US Department of Defense and provides for strong authentication and X.509 path validation with CRL revocation checking. Further, SAML and XACML are among the many other standards provided by Forum Sentry for authentication, authorization, single sign-on, and identity federation.

2.9 Summary
The following items summarize the aspects of service based architecture security.

- **Secure messaging.** Ensure that SOAP messages traversing networks are not viewed or modified by attackers.
- **Protection of resources.** Ensure that individual Web services are adequately protected through appropriate identification, authentication, and access control mechanisms.
- **Negotiation of contracts.** To truly meet the goals of SOA and automate business processes, Web services should be capable of negotiating business contracts as well as the QoP and QoS of the associated transactions.
- **Trust management.** One of the underlying principles of security is ensuring that all entities involved in a transaction trust one another and have established means to build trust relationships through defined standards.
- **Security properties.** All Web service security processes, tools, and techniques rely on secure implementation. A vulnerable Web service may allow attackers to bypass many—if not all—of the security mechanisms discussed in Section 3.

The Forum Sentry™ Security Gateway provides security technology across the diversity of standards for message security, identity, access control, governance, and mediation.
3. Tables of Standards

Forum Sentry™ Security Gateway is a standards-based gateway that was built with the security consideration of FIPS 140-2 compliance and integrity. This provides the industry with a comprehensive, industry-hardened security gateway with out-of-the-box technology to enable business integration and service API exposure with high performance, low-latency throughput of enterprise-class security processing.

3.1 Message Formats and Standards

A summary of the message formats and underlying standards supported by Forum Sentry™ are detailed below.

<table>
<thead>
<tr>
<th>BASE STANDARDS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
<tr>
<td>SOAP 1.1/1.2</td>
<td></td>
</tr>
<tr>
<td>WSDL 1.1, 1.2</td>
<td></td>
</tr>
<tr>
<td>UDDI</td>
<td></td>
</tr>
<tr>
<td>XPath</td>
<td></td>
</tr>
<tr>
<td>XSD, DTD</td>
<td></td>
</tr>
<tr>
<td>XSLT 1.0</td>
<td></td>
</tr>
<tr>
<td>REST</td>
<td></td>
</tr>
<tr>
<td>SwA MIME, DIME, MTOM</td>
<td></td>
</tr>
<tr>
<td>WS-Addressing</td>
<td></td>
</tr>
<tr>
<td>JSON</td>
<td></td>
</tr>
<tr>
<td>AS2</td>
<td></td>
</tr>
<tr>
<td>ebXML</td>
<td></td>
</tr>
<tr>
<td>cXML</td>
<td></td>
</tr>
</tbody>
</table>
### 3.2 Protocol Formats and Standards

A summary of the message formats and underlying standards supported by Forum Sentry™ are detailed below.

<table>
<thead>
<tr>
<th>PROTOCOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HTTP/HTTPS</td>
</tr>
<tr>
<td>• IBM MQ</td>
</tr>
<tr>
<td>• Tibco EMS, Tibco RV</td>
</tr>
<tr>
<td>• Oracle JMS</td>
</tr>
<tr>
<td>• JBOSS JMS</td>
</tr>
<tr>
<td>• ActiveMQ</td>
</tr>
<tr>
<td>• Rabbit MQ</td>
</tr>
<tr>
<td>• AMQP</td>
</tr>
<tr>
<td>• FTP/FTPS</td>
</tr>
<tr>
<td>• SMTP</td>
</tr>
<tr>
<td>• SFTP</td>
</tr>
<tr>
<td>• Inline Protocol Mixing across all protocols</td>
</tr>
<tr>
<td>• Remote Service Endpoint Load Balancing</td>
</tr>
<tr>
<td>• SSL/TLS supported for initiation and termination of all protocols</td>
</tr>
</tbody>
</table>
### 3.3 Identity Formats and Standards

A summary of the identity formats and underlying standards supported by Forum Sentry™ are detailed below.

<table>
<thead>
<tr>
<th>IDENTITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Protocol Level and SOAP/XML Message Level Access Control</td>
</tr>
<tr>
<td>• HTTP Basic Auth, SSL X.509 Mutual Auth, Digest Auth, Cookie, Form Post, Kerberos, SPNEGO</td>
</tr>
<tr>
<td>• WS-Security Auth Username Token, X.509, Kerberos and SAML</td>
</tr>
<tr>
<td>• SAML v1.0, v1.1, v2.0</td>
</tr>
<tr>
<td>• SAML Web SSO (IdP-Initiated and SP-Initiated)</td>
</tr>
<tr>
<td>• OAuth</td>
</tr>
<tr>
<td>• WS-Trust</td>
</tr>
<tr>
<td>• XACML</td>
</tr>
<tr>
<td>• Dynamic any content (header and body) credential extraction</td>
</tr>
<tr>
<td>• Identity Token conversion from any format to any other format</td>
</tr>
<tr>
<td>• Identity Management Integration: CA SiteMinder, LDAP, MS Active Directory, MS ADFS, RSA SecureID, Oracle Access Manager, HP Select Access, IBM TAM, OpenSSO, OpenAM</td>
</tr>
</tbody>
</table>
### 3.4 Security Standards and Features
A summary of the security standards and underlying security features of Forum Sentry are detailed below.

| DATA LEVEL PRIVACY & INTEGRITY | • XML Encryption, XML DSIG, WS-Security Encryption, WS-Security DSIG  
• WS-Security Conversation  
• WS-Reliable Messaging  
• Symmetric Encryption via AES, 3DES  
• One-way hashing via SHA, AES, and SHA-2 algorithms  
• XSD, DTD, and XPath schema validation  
• JSON and XHTML schema and form validation |
| SECURITY | • TCP Layer4-7 Threat Detection and Prevention  
• Web Application Firewall with OWASP Top 10, schema poising, cookie tracking  
• WS-Security 1.1 and 2004  
• SSL v2.0 and v3.0, TLS v1.0, TLS v1.1  
• Denial of Service, Data Leakage, and Malware Detection  
• Integrated On-board Antivirus Engine, BASE64 malware scanning, and ICAP integration |
| CRYPTOGRAPHY & PKI | • Import, Generation and Management of X.509 and PKCS Formats. Direct Java Key Store Import  
• PKCS #1, PKCS #7, PKCS #8, PKCS #11, PKCS #12, X.509 Certificates and CSRs  
• 512- 4096 key sizes. RSA, DSA, DES, 3DES, SHA-1, SHA-2, AES, Elliptical Curve  
• OCSP, CRL via LDAP, XKMS, HTTP, FILE, CDP  
• DoD PKI Certified X509 Authentication with Chain Traversal and CRL checking  
• FIPS 140-2 Level III HSM for Secure Key Storage and Management |
About Forum Systems

Forum Systems, a wholly owned subsidiary of Crosscheck Networks, Inc., is a leader in Service Oriented Architecture (SOA) and secure service mediation. Through comprehensive Threat mitigation and Trust enablement, Forum’s family of hardware, software, and cloud-based instances provides enterprises and government organizations with the foundation for achieving secure service mediation. Processing more than one billion transactions per day worldwide, the FIPS- and DoD-certified Forum products offer the industry’s most comprehensive protection against XML- and SOAP-based vulnerabilities. Forum Sentry has been issued an industry-first patent (7,516,333) for XML security functions such as XML Encryption, XML Decryption, and XML Signatures using a network appliance. For more information, please visit www.forumsys.com.