Model User Guide for Utilizing Web Services to File Certificates of Financial Responsibility

Version 1.0

April 20, 2012

Insurance Industry Committee on Motor Vehicle Administration

Executive Summary

Mandatory liability insurance laws currently exist in 49 of the 50 states. Many jurisdictions require an individual to obtain and maintain certificates of proof of future financial responsibility. An individual may need a certificate of financial responsibility due to unsatisfied judgments, driving without required insurance, convictions of serious moving violations or involvement in a crash and unable to provide evidence of financial responsibility. Certificates of Financial Responsibility are typically referred to as an SR-22, FR-44 or similar designation depending on the jurisdiction and reason for the filing.

Today, few jurisdictions accept Certificates of Financial Responsibility electronically from insurance companies and no standardized methodology exists for the submission of certificates to all the jurisdictions. Jurisdictions accept certificates by numerous methods which include: paper forms via US Mail, faxed forms, emailed, proprietary website entry and costly electronic methods utilizing 3rd party vendors.

Current methods of submission can result in inferior data quality, duplicate entries, and unsatisfactory customer experience. Data quality is affected by the numerous forms of delivery; Duplicate entries are required as insurers must also input data into the insurance company database; Customer experience is affected by delays in delivery to jurisdictions. Also, the submission of certificates via a website does not allow for audit trails by the insurance company.

The purpose of this paper is to propose a standardized method utilizing web services technology to provide certificates of Financial Responsibility to any jurisdiction that requires a certificate. The Insurance Industry Committee on Motor Vehicle Administration (IICMVA) views the use of this technology as the optimum solution for overcoming the limitations of paper Certificates and best meets the needs of all stakeholders. The solution will support numerous state specific data, documentation of insured's compliance related to the Financial Responsibility Laws through a partnership of the jurisdiction, the public, and insurance companies. The method is intended to be uniform, cost effective for the jurisdictions, cost effective for insurance companies, support data security, and beneficial for the public interest. Jurisdictions taking advantage of this technology will eliminate paper processing, reduce manual efforts, and improve data quality.

Foreword

About the IICMVA

IICMVA was formally organized in January 1968. Prior to this time, industry ad hoc committees were assembled as needed by each jurisdiction to assist with the implementation of compulsory insurance and financial responsibility laws.

Ad hoc committees, which operated at the individual state level, were restrictive and inconsistent in function and composition. IICMVA was formed to provide consistent, industry-wide exchange between the insurance industry and all jurisdictions.

IICMVA's basic organization is built around insurers and insurance trade associations. Property Casualty Insurers Association of America (PCI, formerly the National Association of Independent Insurers and the Alliance of American Insurers), the American Insurance Association (AIA), and the National Association of Mutual Insurance companies (NAMIC) comprises the three major trades. Non-affiliated insurers round out the IICMVA roster.

IICMVA is not a lobbying organization. Instead, the Committee serves as a liaison between the insurance industry and state motor vehicle departments in the following subject areas: drivers licensing, vehicle titling/registration, motor vehicle records, compulsory insurance laws, and financial responsibility programs. IICMVA also maintains a close working relationship with the American Association of Motor Vehicle Administrators.

Section One

Introduction to the Model User Guide

Program Goals

The goals for utilization of web services to file Certificates of Financial Responsibility include:

- Support a standardized method for filing Certificates of Financial Responsibility so that most if not all jurisdictions can participate.
- Eliminate paper processing, reduce manual effort, reduce poor data quality
- Improve response time, customer experience and customer privacy
- Provide a guide for electronic filing of Certificate of Financial Responsibility which any jurisdiction can implement.
- Electronic implementation may have an 'up front' cost, but over the long term, manual processing by all parties will be greatly reduced. This is premised on a totally automated process by all parties, with manual intervention on an exception only basis.

User Guide Purpose

The purpose of this guide is to provide insurance companies, jurisdictions, or their respective agents with information needed to file Certificates of Financial Responsibility via web service applications.

This guide provides both business and technical information on how insurance companies may submit Certificates of Financial Responsibility through web services hosted by jurisdictions and/or vendors participating in this web service program. Section one focuses on the general business elements. Section two addresses the technical recommendations and elements to be followed by parties intending to implement this solution.

Note: The guide takes care to provide accurate and informative analysis and information. Until a web service approach for submission of Certificates of Financial Responsibility is fully adopted and implemented in a given jurisdiction, this is merely a guide to potential business and technical aspects for such a system. How a web service system ultimately works depends on state law and implementation. This guide alone should not be relied upon for business or legal decisions nor is it to be considered legal advice.

Program Process Overview

Submission of Certificates of Financial Responsibility by Authorized Insurance Companies and Agents

- A jurisdiction notifies an individual of the need to provide a Certificate of Financial Responsibility for the specified reasons and the individual makes the request of his/her insurance company.
- Each jurisdiction and insurance company is responsible for maintaining a web portal through which the required data on a Certificate of Financial Responsibility can be transmitted from the insurance company to the jurisdiction.
- Valid messages are transmitted from the insurance company to the appropriate department of motor vehicles containing the specified data, using the key information for the Department of Motor Vehicles.
- The messages are transmitted in a standard format established by the industry.

- The insurance company's database maintains a record of having provided the Certificate and continues to monitor its status for the period of time required by the jurisdiction or until such time the policy is terminated.

System Validates Request

The web service application of the participating jurisdiction validates the electronic message received from the insurance company:

- The system verifies that the Certificate of Financial Responsibility is from an authorized insurance company.
- The system verifies that the Certificate of Financial Responsibility has the required message content.
- The system verifies that the message content provided by the insurance company is in the correct format.
- If the message is valid, the jurisdiction then returns an "acknowledgment" transaction and proceeds with processing of the Certificate of Financial Responsibility. If the message is invalid, the jurisdiction will return a response indicating the transaction is invalid and no further processing of the certificate is initiated until a valid message is submitted by the insurance company.

System Distributes Communication

For a valid Certificate of Financial Responsibility, the jurisdiction responds with an electronic message to the insurance company acknowledging receipt of the Certificate.

Program Process Requirements

Business Requirements

The foundation for the process described in Section One of this guide is based on the business, functional, and technical requirements developed by the IICMVA web services business team.

The business requirements were originally identified in the August 16, 2011 IICMVA white paper publication entitled, ***Utilizing Web Services Technology to File Certificates of Financial Responsibility; Version 1.0***.

These business requirements are traceable to the technical specifications outlined in Section Two of this guide. These requirements are complimented by the function and technical requirements also located in Section Two.

The following chart outlines the business requirements referenced:

Business Requirements	
ID #	**Description**
B1	Each participating insurance company will maintain the data necessary to submit required information to the jurisdiction for individual Certificates of Financial Responsibility.
B2	Each jurisdiction will be responsible for maintaining a web service through which online submission of Certificates of Financial Responsibility can be received from individual insurers.
B3	Data needed for the Certificate of Financial Responsibility will be submitted to the appropriate jurisdiction.
B4	The information exchanged will be limited to only those items required to accurately submit the filing.
B5	The certificates will be transmitted in a standard format established by the industry.
B6	A confirmation receipt of filing will be sent back to the submitting party (insurance company or their authorized representative).

Section Two

Technical Processes and Considerations

Technical Overview

In the Executive Summary, an alternative solution to Certificates of Financial Responsibility filings by individual insurance companies through the use of web services was identified. The following is an overview of the standards used to architect this solution. For detailed definitions of these standards and organizations, please refer to the *Glossary* at the end of this document.

Web Services

Web services describe the standardized way that a web user or web-connected program can call another web-based application hosted on a business' web server.

There are two parties involved in the communication, a web service client [request] and the web service [response]. An authorized web user or client can use or "***consume***" the service by submitting a request over the Internet to the web server where the service is located. When called or consumed by a web user or program, the web service fulfills a request and submits the response.

Businesses that host web services are called ***application service providers***. For the Certificate of Financial Responsibility filings, participating jurisdictions serve as the application service providers.

If web services were not available, application service providers would have to offer access to application services from their own enterprise computers. This is a benefit of web services. They are not "hard-wired" to a host entity's file system. Instead, a web service is a program that performs a repeatable task when invoked by an authorized user for a specific purpose.

Used primarily as a means for businesses to communicate with each other and with clients, web services allow organizations to communicate data without intimate knowledge of each others' IT systems behind the firewall.

Open Standards

Web services integrate web-based applications using open standards over an Internet protocol. These open standards include Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Service Description Language (WSDL), Universal Description, Discovery and Integration (UDDI).

Open standards foster the use of common technologies. The following standards bodies are important to keep in mind as they are referenced in this guide:

- *The Web Services Interoperability Organization (WS-I)*
- The *Organization for the Advancement of Structured Information Standards (OASIS)*
- *The World Wide Web Consortium (W3C)*

Internet

The following Internet concepts and terms will be referenced throughout this guide:

- *Transmission Control Protocol/Internet Protocol (TCP/IP)*
- *Hypertext Transfer Protocol (HTTP)*

Security

Security has been the driver behind the kinds of information that companies can readily share through the Certificates of Financial Responsibility filing application. Security specifications are significant points of discussion in this guide due to the nature of the Certificates of Financial Responsibility filings application. The following are important security specifications referenced in this guide:

- *Web Service Security (WS-Security)*
- *Secured Sockets Layer/Transport Level Security (SSL/TLS*)

Functional and Technical Requirements

The following requirements are complementary to the Business Requirements in Section One and provide the foundation for the Technical Specifications in the next section.

Functional and Technical Requirements	
ID #	**Description**
B1	**Each participating insurance company will maintain the data necessary to submit required information to the jurisdiction for individual Certificates of Financial Responsibility.**
B2	**Each jurisdiction will be responsible for maintaining a web service through which online submission of Certificate of Financial Responsibility filings can be received from individual insurers.**
F2.1	Each participating jurisdiction will develop an online system based on web service technology that allows insurance companies to submit Certificate of Financial Responsibility filings.
T2.1.1	The system will be built on an infrastructure (i.e.; ***how*** to send and process a message) based on open standards approved by the World Wide Web Consortium (W3C), WS-I, and OASIS.
F2.2	The system will include enough flexibility in the data elements reported in order to meet the needs of multiple jurisdictions.
B3	**Data needed for Certificate of Financial Responsibility filings will be submitted to the appropriate jurisdiction.**
F3.1	**The jurisdiction will only accept a transmission containing a Certificate of Financial Responsibility filing which has a valid verification key.**
F3.2	**The verification key will consist of an authentication key and a message content key.**
T3.2.1	**The authentication key will include an X.509 certificate.**
T3.2.2	**The message content key from the requesting party will include the following mandatory and conditional data elements:** **Owner/Operator Driver's License** **Owner/Operator Last Name** **Owner/Operator Date of Birth**

Functional and Technical Requirements	
ID #	**Description**
B4	**The information exchanged will be limited to only those data elements required to accurately submit the filing.**
F4.1	The endpoint will be determined through the use of a two character postal abbreviation filing state code as a routing key in a point to point transaction.
B5	**The certificates will be transmitted in a standard format established by the industry.**
F5.1	The system will incorporate basic web service infrastructure standards.
F5.2	The system will read or interpret the business contents of the filing message (or payload) based on a common standard schema.
T5.2.1	The common standard schema chosen will have an approach to align with the other web service infrastructure standards.
F5.3	The system will be based on one set of web service security standards that will be used by all participating jurisdictions.
F5.4	Jurisdictions will develop the system based on one set of authentication standards.
B6	**A confirmation receipt of filing will be sent back to the submitting party (insurance company or their authorized representative).**
F6.1	The jurisdiction will respond with an acknowledgement to the insurance company verifying receipt of the transaction.
F6.2	If the insurance company does not receive the acknowledgement, it is assumed that the insurer will rely on its current follow-up procedures.

Data Dictionary

While the following data dictionary provides some level of data element detail, a complete reference document that describes the relationships of all data elements contained in the online Certificates of Financial Responsibility filing messages can be obtained by contacting the Accredited Standards Committee (ASC X12) at http://www.x12.org/.

Category	Data Element Name	Data Element Description	Sample Content	Data Type	Mandatory Optional Conditional
Sender Information	NAIC	Insurance Company	12345	String	M
Receiver Information	Name	Organization Name	ST DMV	String	O
	Identifier	Organization Identifier	12345	String	M
Transaction Information	Case Number	Unique identifier assigned by the sender.		String	O
	Transaction Purpose	Code identifying the purpose of the Document.	**FR2** **FR44** **FR46** **S22A** **S22B** **S22C** **S22D** **S26** **SR1A** **SR1P** **SR21** **SR22** **SR22A** **SR23** **SR24** **SR26** (Refer to Appendix B for code value descriptions)	String	M

	Transaction Type		**VSP** = Vehicle Specific Personal **NSP** = Non Vehicle Specific Personal **VSC** = Vehicle Specific Commercial **NSC** = Non Vehicle Specific Commercial **O** = Owner **P** = Operator **OP** = Owner & Operator **B** = Broad **Z** = Low Cost	String	M
	Transaction Effective Date		ccyy-mm-dd	Date	M
Policy Information	Policy Number	Policy Number	123456789	String	M
	Effective Date	Policy effective date	ccyy-mm-dd	Date	O
	Expiration Date	Policy end date	ccyy-mm-dd	Date	O
Insured Information	Prefix	Title before individual's name		String	O
	First Name	First name of operator.		String	M
	Middle Name	Middle name of operator.		String	O
	Last Name	Last name of operator.		String	M
	Suffix	Abbreviated Name Suffix (JR, SR, etc…)		String	O
	Date of Birth		ccyy-mm-dd	Date	C
	Federal Tax ID or SSN	Social Security Number (Numeric values only - omit all other characters)	123456789	Numeric	O

	Driver's License	The unique number assigned to an individual by each U.S state's Department of Motor Vehicles.	123456789	String	C
	Driver's License State	Two-character postal abbreviation state code for driver's license issuing state		String	O
	Street Address			String	O
	City			String	O
	Country Subdivision	State or Province		String	O
	Postal Code	Zip Code		Numeric	O
Vehicle Information	VIN	Vehicle Identification Number	XYZ123ABC1234567	String	O
	Make	Vehicle Manufacturer		String	O
	Model	Vehicle Model Name		String	O
	Year	Vehicle Model Year (CCYY)		Numeric	O

Jurisdiction's Responsibilities

The business and technical specifications require that each participating jurisdiction develop a Certificate of Financial Responsibility web service. The following information explains the technical specifications behind this requirement in more detail.

Build and Maintain a Web Service and Common External Interface

Each participating jurisdiction must design, develop, and maintain a web service capable of receiving electronic Certificates of Financial Responsibility. Each jurisdiction's web service ***must*** have a common, or standard, external interface. Standard interfaces are crucial because they allow the receipt of standard filings from participating insurance companies, reducing the time and cost of maintenance.

Web services developed by jurisdictions will adhere to the ***SOAP 1.1 open standards***. SOAP 1.1 standards provide a foundation for building web services, and they are widely supported by many computing platforms. Other web service standards, such as WS-Security, are built upon the SOAP 1.1 specification.

Leveraging industry standards enables all jurisdictions to create a standard external interface. Such a common interface allows each jurisdiction to develop just one web ***service client*** to interact with each participating insurance company.

Distribute the WSDL File Accordingly

The common external interface previously discussed is a collection of ***method signatures*** which define what the web service is capable of doing and where it may be accessed. These method signatures are described in a file written in the Web Services Description Language (WSDL), an XML-based language. (Sometimes a WSDL file is simply referred to as a company's "WSDL," pronounced "***wizdle***.")

Other than the ***Uniform Resource Locator (URL address),*** or endpoint, of the web service, each participating jurisdiction's WSDL should look similar.

If a jurisdiction changes the location of its web service, it is the responsibility of that agency to provide all insurance companies with the updated endpoint.

Each participating insurance company will retrieve the endpoint for the appropriate jurisdiction via another location, such as a local configuration file. According to industry recommendations, it is more efficient to utilize a single WSDL file and store the endpoint elsewhere, rather than manage multiple WSDL files.

Secure the Web Service

Any type of application service available on the public Internet needs to be secured to prevent certain exposures. Protecting a jurisdiction's technical infrastructure and data is a primary concern. Therefore, appropriate measures must be taken to prevent unauthorized requesting parties from accessing the jurisdiction's data.

There are a number of options for securing a web service. Regardless of the security solution, IICMVA recommends the use of industry standards. Using industry standards provides companies with the ability to secure their web services while maintaining a level of consistency and flexibility to support multiple platforms (e.g., UNIX or Windows) and application server platforms (e.g. Java and .Net). Using industry standards should also help to position ourselves for potential changes or modifications due to the evolution of technology.

Transport Level Security

For Transport Level Security, insurance companies will use ***SSL 3.0*** for mutual authentication. SSL 3.0 enables requesting parties to know they are communicating with the correct jurisdiction. In turn, SSL 3.0 with client authentication allows a jurisdiction to know it is communicating with the correct authorized party.

SSL also provides a secure, or encrypted, channel for applications to communicate with each other, eliminating the need to encrypt data at the application level which could potentially cause performance degradation.

SSL with client authentication requires jurisdictions to register and obtain a public/private key certificate pair, otherwise known as ***X.509 certificates.*** Under this scheme, the jurisdiction must trust the requesting party's certificate, and the requesting party must trust the jurisdiction's certificate. Each insurance company will be responsible for providing the jurisdiction with a copy of their public certificate.

A Class 3 certificate is typically used for business transactions and is required by IICMVA due to its level of integrity compared to Class 1 and 2 certificates.

This requires that all Class 3 certificates are purchased from trusted distributors. The following table represents some commonly trusted certificate authorities.

Certificate Authority	Website
Verisign, Inc.	http://www.verisign.com
Entrust	http://www.entrust.com/digital-certificates
Thawte	http://www.thawte.com

Insurance Company's Responsibilities

It is the responsibility of participating insurance companies to develop a Certificate of Financial Responsibility web service client that is based on the standards identified in the sections above. The following information explains the technical specifications behind this requirement in more detail:

Collect the Key Information Needed to Submit Certificate of Financial Responsibility filings

Each insurance company must determine how it will collect basic information needed to submit a standardized Certificate of Financial Responsibility filing.

Build and Maintain a Web Service Client

The insurance company must develop a web service client capable of sending a Certificate of Financial Responsibility filing to a jurisdiction's web service. Each insurance company's web service client must provide the required information necessary to invoke a request and electronically file a policyholder's insurance information.

The web services developed by the insurance companies will adhere to the SOAP 1.1 standards. Therefore, the receiving party's web service client must use SOAP 1.1 standards as well. Fortunately, most application development tools provide a framework that supports the standards identified in this model implementation guide.

Manage One Common WSDL File

Each insurance company that develops a web service application will adhere to the schema chosen. Therefore, these companies have a much easier task of managing a single WSDL file necessary for the client to understand the input requirements of the web service. In addition, insurance companies will need to store an endpoint indicating the location of each state's web service. Without the endpoint, no communication can take place.

In theory, one third party vendor or agent could store and maintain a single web service client and the endpoint for each participating jurisdiction. However, due to the risk of exposing each service endpoint, IICMVA recommends that each insurance company host its own web service client and manage all endpoints.

Route the Request to the Appropriate Jurisdiction

As previously noted, the endpoint tells the web service client where to send a request. However, the client still needs to know what endpoint to look up. Therefore, the filing party's application should contain logic that correlates a state abbreviation code with the appropriate endpoint record.

Maintain and Store Access Credentials

Since the Certificates of Financial Responsibility filings web service will support mutual SSL with client authentication, it is necessary for the requesting party to obtain an X.509 certificate key pair from a trusted distributor, such as Entrust or Verisign. Companies that distribute certificates have a "Trusted Root Certificate". All keys signed by that root certificate trust each other.

It is absolutely necessary for each company to keep its private key protected from any unauthorized person. As a security measure, all certificates expire after a period of time, typically 2 years. Once the certificate has expired, it will no longer be accepted as a valid authentication token. Therefore, it is necessary for each requesting party to maintain a valid certificate and provide participating jurisdictions with renewed certificates as soon as possible.

The following benefits outweigh the maintenance concerns when using certificates:

- Certificates are more secure than username and password schemes.
- Certificates are easy to implement and use.
- The same public certificate sent for transport level authentication can be sent in the message level.

XML Payload Message

XML messages for online insurance verification have been independently developed by the ***Accredited Standards Committee (ASC X12)*** and the ***Association for Cooperative Operations Research and Development (ACORD).***

At this time, only ASC X12 has developed an XML schema that IICMVA can reference in this guide.

Service Level Agreements (SLA) and Volume Metrics

It will be the responsibility of the jurisdictions to abide by the Service Level Agreement (SLA) established with insurance companies. Each company and jurisdiction will have different business volume metrics; therefore, both parties will need to build an infrastructure that allows for compliance with the established SLA.

The Service Level Agreement is composed of the following areas:

System Availability

Each jurisdiction shall assume the responsibility to provide a high availability online system able to receive Certificate of Financial Responsibility filings. As with all systems, a reasonable amount of down time is expected to maintain company systems, commonly referred to as "planned system outages".

IICMVA recommends that each jurisdiction provide their respective online availability hours to participating insurance companies.

Testing Period

An appropriate amount of lead time for implementation and testing should be provided in advance of implementation of the Certificate of Financial Responsibility filing program. IICMVA recommends a testing period of no less than nine months be established to provide that insurance companies and jurisdictions can ensure a fully functional Certificate of Financial Responsibility filing program.

Implementation Processes and Testing Strategy

To ensure a consistent quality product across companies and jurisdictions, the IICMVA recommends that a standard testing strategy and implementation process be utilized. For the initial implementation, the testing strategy and implementation process checklist are presented in Appendix A. This document may be modified and updated to meet the needs of the system as it is enhanced.

APPENDIX A

Implementation Processes and Testing Strategy for Insurance Certificates of Financial Responsibility filings

Test Strategy

Test Objectives

- Verify that the requesting party is able to send a valid XML message
- Verify that the receiving party is able to receive and respond with a valid XML message
- Verify that appropriate responses are provided for business scenarios

Test Approach

1. **Schema Validation**
   a. Requesting party sends receiving party a sample request XML message via e-mail. Each party will validate the XML messages against their WSDL.
   b. The receiving party provides the response XML message back to the requesting party via email.
2. **Functionality Testing (Test Environment)**
   a. Receiving party will provide test cases to the requesting party.

   For all levels and types of tests, test cases will require, but not be limited to the following data elements:

   - **Owner/Operator Driver's License**
   - **Owner/Operator Last Name**
   - **Owner/Operator Date of Birth**

   b. Functionality testing will be conducted for various business scenarios based on the test cases.
3. **Performance Testing (Test Environment)**
   a. If required by the requesting party, performance (load) testing must be done in a test environment.
   b. The number of transactions and the amount of testing time should be agreed upon by both parties.
4. **Production Checkout (Production Environment)**
   a. Receiving party will provide test cases to the requesting party.
      i. For all levels and types of tests, test cases will require, but are not limited to the following data elements:

      - **Owner/Operator Driver's License**
      - **Owner/Operator Last Name**
      - **Owner/Operator Date of Birth**

b. The requesting party may develop a series of test cases with data relevant to the receiving party to be used during the production checkout.

c. Functionality testing will be conducted for various scenarios based on the test cases.

Setup Checklist (completed prior to testing)

1. The insurance company purchases certificates (See Transport Level Security information in Model User Guide) – A Class 3 certificate is typically used for business transactions and is recommended by the IICMVA due to its level of integrity. This requires that Class 3 certificates be purchased from trusted distributors.

2. The jurisdiction (or its appointed representative) and insurer will exchange networking essentials including; source IP addresses for entities (Test, Production or both), destination endpoints (complete URL) as well as a public certificate provided by the insurance company to be used for Authentication/Authorization/Accounting.

3. If required, the jurisdiction (or its appointed representative) and the insurer will open firewall ports at their end to establish the two- way communication.

4. Checkout is performed for TCP/IP network connectivity between the state jurisdiction (or its' appointed representative) and the insurer. This does not include web service functionality at this point. The jurisdiction shares the IP address and certificate authorities.

5. The insurance company provides the jurisdiction with their organization name which is included in the XML message. The jurisdiction includes these details in their database to validate that the insurance company is considered a valid requesting party.

APPENDIX B

Schema

Refer to ASC X12 or ACORD.

Transaction Codes - Descriptions

Code	Description
FR2	FL only - SR22 for PIP and PDL coverages only
FR44	Financial Responsibility filing indicating increased coverage is in force
FR46	Financial Responsibility filing indicating increased coverage is no longer in force
S22A	SC only - Non-restrictive SR22
S22B	SC only - Non-owner SR22
S22C	SC only - Restricted SR22
S22D	SC only - Motorcycle SR22
S26	SC only - Cancels S22A, S22B, S22C, or S22D
SR1A	CA only - Verification of coverage for an accident where damage total is > $750
SR1P	CA only - Verification of coverage for an accident
SR21	Notice of liability insurance
SR22	Financial Responsibility filing indicating coverage is in force
SR22A	IL Only - Financial Responsibility filing indicating coverage is in force
SR23	Financial Responsibility filing indicating coverage is in force for fleets
SR24	Notice of change of vehicle to update a previously filed SR22
SR26	Financial Responsibility filing indicating coverage is no longer in force

GLOSSARY

- ***Extensible Markup Language (XML)*** is a flexible way to describe data and the format of that data over the Internet. XML allows systems designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and organizations. For online insurance Certificates of Financial Responsibility filings, the data exchanged in the coverage request and response would be "tagged" in XML. Sometimes developers refer to this data as the ***"XML payload message."***

  XML schemas for online insurance Certificates of Financial Responsibility filings have been independently developed by the ***Accredited Standards Committee (ASC X12)*** and the ***Association for Cooperative Operations Research and Development (ACORD).***

- ***High Availability*** A software application that is scheduled to be available to users with only minimal scheduled or planned system outages.

- ***Hypertext Transfer Protocol (HTTP)*** is the set of rules that define how messages are formatted and transmitted over the Internet. HTTP defines what actions should be taken by web servers and browsers in response to various commands. HTTP runs on top of the TCP/IP suite of protocols.

- The ***Organization for the Advancement of Structured Information Standards (OASIS)*** is a not-for-profit, global consortium that drives the development, convergence, and adoption of e-business standards.

- ***Planned System Outages*** are schedule maintenance periods for system backup, repair and upgrade operations.

- ***Real Time*** is a form of synchronous transaction processing in which each transaction is executed as soon as complete data becomes available for the transaction with no significant time delay. Real time is a description of a process, not a description of the accuracy of the expected result of that process

- ***Issuing Party*** can be an insurance company or their authorized vendor with whom they have contracted to act on their behalf.

- ***Secured Sockets Layer/Transport Level Security (SSL/TLS***) uses certificates to authenticate the identity of the endpoints, or ***"sockets,"*** of a trusted session or message transmission (i.e.; ***transport level authentication***). TLS is derived from SSL and has succeeded SSL as the protocol for managing the security of a message over the Internet.

  SSL and TLS are integrated into most web browsers and servers, but they are not interoperable. However, a message sent with TLS can be handled by a web browser or server that uses SSL, but not TLS.

  SSL/TLS runs between the HTTP and TCP/IP layers.

- ***Simple Object Access Protocol (SOAP)*** is used to transfer XML payload messages or data. SOAP allows programs running in the same or different operating systems to communicate with each other using a variety of Internet protocols such as Simple Mail Transfer Protocol (SMTP), Multipurpose Internet Mail Extensions (MIME) and ***Hypertext Transfer Protocol (HTTP).*** SOAP messages are independent of any operating system or protocol. This guide will focus on HTTP.

  Specifically, SOAP is a lightweight XML-based messaging protocol used to encode the information in web service request and response messages before sending them over a network. Simply put, SOAP serves as the envelope that wraps around the XML payload message, and it glues together

different computing systems so companies can interact with each other. Some refer to it as the SOAP ***"wrapper."***

- ***Transmission Control Protocol/Internet Protocol (TCP/IP)*** is the basic two-layer suite of communication protocols, ***or rules***, used to connect hosts on the Internet.

  The TCP layer breaks down a message file into smaller units of data called a ***packet*** and transmits that packet over the Internet to another TCP layer. The receiving TCP layer reorganizes the data into the original message file.

  The IP layer serves a postal function as it ensures the packet reaches the correct address or destination on the Internet. This destination is sometimes referred to as the ***IP address***.

- ***Universal Description, Discovery, and Integration (UDDI)*** is an XML-based, distributed directory that enables businesses to list themselves on the Internet and discover each other, similar to a traditional phone book's yellow and white pages. WSDL is the means used to identify services in the UDDI registry. UDDI is used for listing what services are available.

- ***Unplanned System Outages*** are the result of uncontrollable, random systems failures associated with faults or defects with software or hardware components.

- ***Web Services Description Language (WSDL)*** is an XML-based language used to describe a web service's capabilities as collections of communication endpoints capable of exchanging messages. In other words, WSDL describes the business services offered by an application service provider and the way other businesses can electronically access those services.

- ***The Web Services Interoperability Organization (WS-I)*** is an industry group that ensures web service specifications are compatible and interoperable across platforms, operating systems, and programming languages. WS-I has captured its interoperability research in a document called the ***WS-I Basic Security Profile 1.0***.

- ***Web Service Security (WS-Security)*** is a security specification that encrypts information and ensures that it remains confidential as it passes between entities. ***Authentication*** is the process of verifying the identity of a person or entity. For online Certificates of Financial Responsibility filings, this person or entity would be the requesting party.

  WS-Security provides authentication at the message level (i.e.; ***message level authentication***), and it was developed by OASIS.

- ***The World Wide Web Consortium (W3C)*** is an international consortium of companies involved with the Internet to develop open standards so that the web evolves in a single direction rather than being splintered among competing factions.

Summary of Revisions

Bibliography

Bulkeley, William M., "Microsoft, IBM Set Standards Pact,"
The Wall Street Journal, September 2003, Technology Journal Section, cols. 3-5.

Fletcher, Peter and Mark Waterhouse, Web *Services Business Strategies and Architectures,*
Birmingham: Expert Press, 2002.

Gruman, Galen, "Getting Ready for Web Services,"
CIO, March 1, 2003, pp. 94-98.

IICMVA Web Service Business and Technical Subcommittee Teams.

Jones, A. Russell, "The 10 Technologies That Will Help You Stay Employed,"
DevX, (Internet), December 11, 2002.

MacSweeney, Greg, "Web Services: Here To Stay?"
Insurance & Technology, September 2002, pp. 53-55.

Olavsrud, Thor, "Microsoft, IBM Set Web Services Standard Pact,"
Internet News, (Internet), September 18, 2003.

Rescorla, Eric, *SSL and TLS: Designing and Building Secure Systems*,
Boston: Addison-Wesley, 2003.

Thing, Lowell (Founder) and Ivy Wigmore (Site Editor), *WhatIs.com* (Internet Education Tool),
Solely owned and copyrighted by TechTarget, Inc.

Wong, Wylie, "Microsoft and IBM Sign Web Services Pact,"
ZDNet US, (Internet), August 9, 2002.