# Model User Guide for Implementing Online Insurance Verification

***Using Web Services to verify evidence of auto liability insurance***

***Version 4.0***

***August 25, 2010***


Insurance Industry Committee on Motor Vehicle Administration

# Executive Summary

Mandatory liability insurance laws exist in 49 of the 50 states. Auto Liability Insurance Reporting (ALIR) programs, often referred to as State Reporting systems, are designed to enforce compulsory insurance laws in 32 states.

From an insurance company perspective, evidence suggests that state reporting programs have not effectively met their main objective: to identify and track uninsured motorists. These programs are costly, difficult to implement, hard to maintain, and a burden for insured drivers.

Recent and ongoing advances in technology, such as Web services and Internet-based transaction processing provide insurance carriers with an opportunity to provide online verification of evidence of auto insurance to state jurisdictions.

These technological developments offer many benefits and reduce detriments to all stakeholders concerned with enforcing mandatory liability insurance laws. The Insurance Industry Committee on Motor Vehicle Administration (IICMVA) believes that Web service technology is a solution to address the need by state agencies to verify evidence of auto insurance.

# 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 state 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 state 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) comprise 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.

## *Business Direction*

Technology has evolved significantly since the late 1950s when states began enforcing their compulsory automobile liability insurance laws. Paper verifications were followed by tape-based cancellation reporting systems. Eventually, electronic reporting came into use.

Today, however, we are in an age of Internet-based, shared services. Businesses will increase their use of Web services defined by *The Wall Street Journal* as "software that many computer experts believe will usher in a new era of secure but simple interconnections among computer systems at different companies."[1]

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

*IICMVA views the use of this technology as the best way to resolve what has become a controversial public policy issue: enforcement of mandatory or compulsory insurance laws.*

Enforcement of mandatory or compulsory insurance laws should be limited to event-based situations. Examples of these events could be, but are not limited to: vehicle registrations, traffic stops or accidents. If a jurisdiction desires additional pre-emptive enforcement, that enforcement should be by a random sample verification of insurance by the appropriate government department.

Secured Web applications make event-based verification of evidence of insurance both possible and desirable. Accessing data to conduct business is nothing new to consumers who regularly bank, shop, or bid over the Internet. It is also nothing new to jurisdictions which disseminate information, collect citizen input, and conduct the business of state government over the Internet. Giving jurisdictions the capability of verifying evidence of insurance in a secured Web environment is an extension of this concept.

On September 17, 2003, IBM and Microsoft announced that they had come to an agreement on software standards for Web services; therefore, the ability to integrate systems among different trading partners could soon be a reality in the realm of insurance verification.[2]

IICMVA believes the industry must respond to this technological opportunity to advance the effectiveness of insurance verification programs.

## ***Vision***

The Committee strongly supports an event-based, online inquiry approach to evidence of insurance verification.

*IICMVA's vision includes simple online applications that can support single policy inquiries. This vision incorporates the use of true Web services that can support the interconnection of systems between authorized trading partners, namely insurance carriers and state agencies.*

An online inquiry approach to verifying evidence of insurance provides many benefits:

- Jurisdictions can obtain the documented ***online status*** of insurance information at any point in time within certain business constraints.

  ***Note:*** Insurance verification Web services can only verify ***issued policies***, not applications. Therefore, online status refers to the information readily available on an insurance carrier's internal databases at a given point in time. When an authorized inquiry is received, an insurer can only respond as soon as possible upon the effective date of a policy.
- Jurisdictions can incorporate online verification systems into their license plate renewal programs.
- There is no need to exchange massive amounts of data that is rarely, if ever, referenced, let alone 100% accurate and/or timely.
- The confidentiality of insurance information is protected within the confines of each insurance carrier's IT environment.
- The matching limitations and data integrity issues of current state reporting programs are reduced.
- Customer service is improved because primary search criteria are based on the business rules within each company.
- Commercial insurance carriers are in a better position to comply with state mandates.
- Carriers can realize the cost effective use of resources since an inquiry system can be built one time for all states, leaving room for simple upgrades as future needs arise.

[2] Thor Olavsrud, "Microsoft, IBM Set Web Services Standard Pact." *Internetnews.com*, September 18, 2003, Enterprise Section, Jupitermedia Corporation.

- Privacy is protected: Only designated, legally authorized entities will have access. The information provided is very limited and state of the art technological safeguards, such as the latest methods of encryption, are included.

IICMVA believes that Web service technology is a solution to address the need by state agencies to verify evidence of minimum financial responsibility coverage.

# Table of Contents

# Section One

## Introduction to the Model User Guide

### Program Goals

The goals for online insurance verification via Web services include:

- Providing an accurate, flexible, and simple method for providing verification of evidence of auto liability insurance that will improve customer service.
- Developing a standardized program that can be used by all states.
- Improving data security since detailed policy information will not be transmitted between participants.

### Program Purpose

The purpose of online insurance verification is to assist in the enforcement of motor vehicle liability insurance requirements.

Other state reporting models require insurance carriers to report insurance information which is then compared to vehicle registration data maintained by motor vehicle departments. Under the reporting model, any vehicle registrations not tied to an insurance record are considered uninsured. Unfortunately, data integrity problems inherent to the reporting process make it an inaccurate method of verifying evidence of insurance. Repeated exchanges of data between insurers and jurisdictions in an attempt to match information, is a time consuming process that often does not result in a positive resolution.

IICMVA offers an approach that differs from state reporting: ***online insurance verification or inquiry via Web services.***

Utilizing the online insurance inquiry model, the presence of minimum financial responsibility evidence may be verified when a requesting party is presented with a financial responsibility event.

Online verification bypasses the need to identify a match between the insurance carrier and motor vehicle department information. Instead, a real time response can be provided to an insurance inquiry that contains standardized request information. More importantly, an accurate response can be provided.

Online verification allows requesting parties to go directly to the source of insurance information – the insurance companies themselves.

**Note**: The IICMVA recognizes that business models for insurance verification may vary to some degree for each state jurisdiction. If a state jurisdiction determines there is a need for insurance carriers to provide the jurisdiction with additional insurance information, the IICMVA provides guidance for this process, described in the IICMVA publication titled “Insurance Data Transfer Guide”.

### User Guide Purpose

The purpose of this guide is to provide insurance companies, state jurisdictions, or their respective agents with information needed to conduct online verification of evidence of auto financial responsibility via Web service applications.

This guide provides both business and technical information on how ***requesting parties*** (e.g., motor vehicle departments) may submit insurance verification requests to Web services hosted by insurance carriers participating in this web service program. The first section will focuses on the

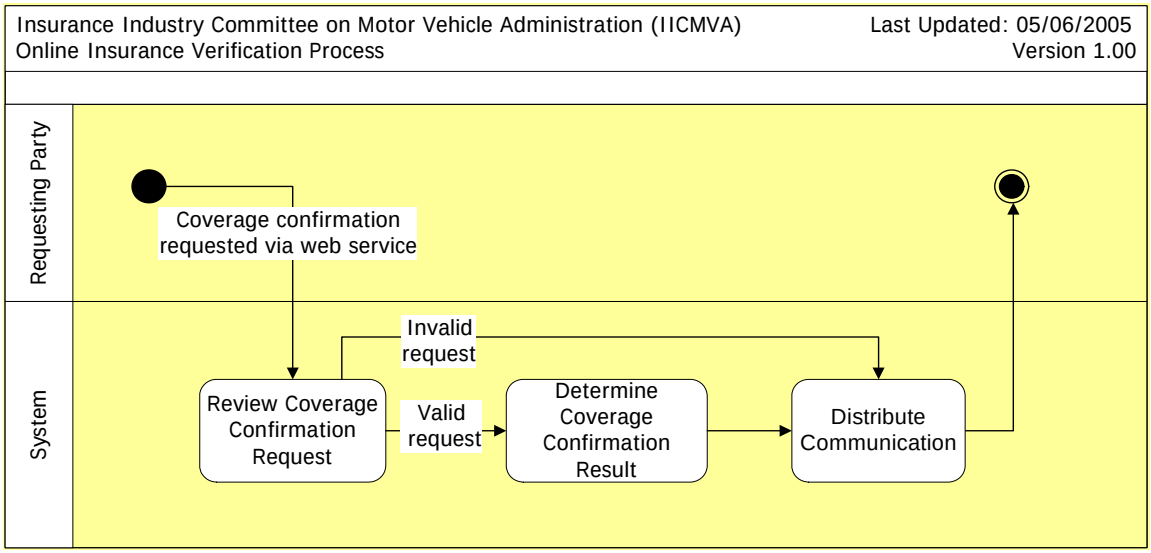
general business elements. Subsequent sections will address the technical recommendations and elements to be followed by parties intending to implement this solution.

Note: The guide takes care to provide accurate and informative analysis and information. Nonetheless, until a Web Service approach to verification 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. Consequently this guide alone should not be relied upon for business or legal decisions nor is it to be considered legal advice.

### Program Overview

When presented with a financial responsibility event, the requesting party simply submits a standardized, ***request for evidence of insurance*** to the Web service of a participating insurance carrier. In turn, the insurance carrier replies with a standardized, ***evidence of insurance confirmation response***.

The following swim lane diagram has been provided to illustrate the inquiry and response process:




***Note:*** The insurance company's response indicates whether it can confirm minimum financial responsibility insurance is present on a date in question. *It does not identify the minimum financial responsibility limits that are present on an insurance policy or substitute for an insurance company's claims handling function since it is not able to confirm an insurance carrier's liability for any claim in question.*

## Program Process Overview

### Authorized Requesting Party Submits Evidence of Insurance Verification Request

An authorized requesting party submits a request or inquiry to verify evidence of insurance to the insurance verification Web service application of a participating auto insurance carrier.

The request will be sent in an XML payload message. The message content key from the requesting party shall include ***mandatory*** data elements (Functional and Technical Requirements T3.2.2).

The message content key from the requesting party may include ***optional*** data elements (Functional and Technical Requirements T3.2.3).

*Note: Versions evolve over time due to changing business requirements and the requirements of the Standards organizations. Please refer to the Standards organizations for the most up-to-date request codes and their values.*

See Appendix B for request codes and corresponding values.

### System Validates Request

The Web service application of the participating insurance carrier validates the request to verify the evidence of minimum financial responsibility insurance:

- The system verifies that the verification request is from an authorized requesting party.
- The system verifies that the verification request has the required message content or policy information.
- The system verifies that the policy information provided by the verification request is in the correct format.

If the request is ***invalid***, the system responds with the following ***result***: ***UNCONFIRMED.***

**UNCONFIRMED** results for invalid verification of evidence of insurance requests may be supplemented with ***reason messages*** available from the ANSI X12/XML or ACORD standard specifications.

The descriptions and code values for the **UNCONFIRMED** reason message that may be optionally returned for an invalid request may vary, depending upon which version of the XML Schema an insurer has elected to utilize.

*Note: Versions evolve over time due to changing business requirements and the requirements of the Standards organizations. Please refer to the Standards organizations for the most up-to-date reason message descriptions and code values.*

See Appendix B for response codes and descriptions (represented in red).

If the request is ***valid***, the Web service application continues with the verification process and attempts to determine if minimum financial responsibility insurance is present.

### System Determines Verification Result

The Web service application takes the valid request and evaluates whether evidence of insurance can be verified for the date specified in the inquiry:

- The system evaluates whether the policy information provided in the verification request is present on the insurance carrier's database.
- The system determines if minimum financial responsibility insurance was present and the policy was active on the requested verification confirmation date.

### System Distributes Communication

For valid evidence of insurance verification requests,

If minimum financial responsibility insurance was present and the policy was active on the requested verification date, the system responds with the following ***verification result***: ***CONFIRMED.***

If minimum financial responsibility insurance was not present and the policy was not active on the requested verification date, the system responds with the following ***verification result***: ***UNCONFIRMED.***

The term **UNCONFIRMED** does not necessarily mean there is no minimum financial responsibility insurance available on a policy record. **UNCONFIRMED** could also mean the insurance carrier could not find any information with the input provided. It is important that authorized requesters enter accurate input.

**UNCONFIRMED** results for valid verification requests may be supplemented with ***reason messages*** available from the ANSI X12/XML or ACORD standard specifications. Please refer to those standards bodies for the most up-to-date available ***reason messages***.

The decision to accompany an **UNCONFIRMED** response with reason messages and which messages are returned are made independently by each insurer. Proprietary business rules of each insurer also determine which reason messages, if any, are used. See Appendix B for response codes and descriptions (represented in blue).

> ***Note:*** *It is important to note that IICMVA gave a great deal of consideration to the type of response provided by the Web service application described in this guide.*
>
> *Due to privacy concerns, it was decided that detailed policy information could not be a part of the verification result since it would have to travel over the public Internet. However, the verification result does provide what is most important: verification of auto financial responsibility insurance based on the minimum financial responsibility limits required by each state. Financial responsibility limits will not be passed back to the requesting party because internal rules should take the state code of the requesting party into consideration when verifying minimum financial responsibility limits for each state.*
>
> *The Web service application bypasses the need to transport vast amounts of data. In addition, the application enables requesting parties to confirm evidence of insurance in an online environment directly with the source of the policy information—the insurance carrier.*
>
> *IICMVA believes this is a more accurate approach.*

# Program Process Requirements

## Business Requirements

The foundation for the inquiry 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 March 2004 IICMVA white paper publication entitled, ***Online Insurance Verification – Using Web Services to Verify Auto Insurance Coverage Version 1.0***: http://www.iicmva.com/websvc.pdf.

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 verify the evidence of insurance provided to their own customers. |
| B2 | Each insurance company will be responsible for maintaining a Web service through which online insurance verification can take place by trading partners. |
| B3 | Valid verification inquires will be made using key information to route a request to the appropriate carrier for a response. |
| B4 | The information exchanged will be limited to only those items needed to accurately route the request and confirm evidence of insurance, keeping any privacy concerns to a minimum. |
| B5 | The sources of the data can vary, as long as they are transmitted in a standard format set by the industry. |
| B6 | Confirmation of evidence of insurance will be sent back to the requesting party for appropriate action. |

# Section Two

## Technical Processes and Considerations

### Technical Overview

In Section One, "Introduction to the User Guide - Program Purpose", an alternative solution to insurance verification by the individual state 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 insurance verification application, participating insurance carriers would 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 company'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 carriers can readily share through the online insurance verification application. Security specifications are significant points of discussion in this guide due to the nature of the insurance verification 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 company will maintain the data necessary to verify evidence of insurance for its own customers.** |
| **B2** | **Each insurance company will be responsible for maintaining a Web service through which online insurance verification can take place by trading partners.** |
| F2.1 | Each participating insurance company will develop an online, insurance verification system based on Web service technology that authorized state or federal agencies can use to inquire about minimum financial responsibility insurance. |
| 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 to allow for additional data elements if other trading partners want to access the system in the future. |
| T2.2.1 | The inquiry must come from known, authorized trading partners. |
| F2.3 | The system will allow individual policy number searches on individual customer records. |
| F2.4 | The system will allow multiple policy number searches on multiple customer records. *(**Note:** This is not a batch processing requirement.)* |
| F2.5 | The System will provide high availability. **See the Service Level Agreement (SLA) for System Availability within this document.* |
| F2.6 | The system will provide the quickest response time possible during the busiest hour of the day while the system is under load. **See the Service Level Agreement (SLA) for Response Time within this document.* |
| **B3** | **Valid verification inquiries will be made using key information to route a request to the appropriate carrier for a response**. |
| F3.1 | Carriers will individually decide at what level they will verify evidence of insurance to a requesting party: *policy level* or *vehicle level*. |

| Functional and Technical Requirements | |
|---|---|
| **ID #** | **Description** |
| F3.2 | The system will only accept an inquiry that has a valid verification key before it will perform an inquiry. |
| F3.3 | The verification key will consist of an authentication key and a message content key. |
| T3.2.1 | The authentication key will include an authorized user code. |
| T3.2.2 | The authorized user code will be present first before the system will perform an inquiry based on the message content key. |
| T3.2.3 | The message content key from the requesting party will include the following mandatory data elements: Policy Key<br>***Note:*** *The policy key for each insurance carrier may be a carrier's policy number, or a number that a carrier uses internally to locate a policy record.*<br>• Vehicle Identification Number (VIN)<br>***Note:*** *VIN is used by carriers that will verify evidence of insurance at the vehicle level. Some carriers may choose to confirm insurance at the policy level.*<br>• NAIC (National Association of Insurance Commissioners) Code<br>• Requested Verification Effective Date |
| **B4** | **The information exchanged will be limited to only those items needed to accurately route the request and response messages, keeping any privacy concerns to a minimum.** |
| F4.1 | A legal trading partner agreement between insurance carriers and the requesting party will be required to exchange data via the Web Service. |
| F4.2 | The requesting party will be responsible for determining the appropriate company to which it will send a request. |
| F4.3 | The endpoint will be determined through the use of the NAIC identifier as a routing key in a point to point transaction. |
| **B5** | **The sources of the data can vary, as long as they are transmitted in a standard format set 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 an inquiry message (or payload) based on one common XML standard. |
| T5.2.1 | The common XML standard chosen will have an approach to align with the other Web service infrastructure standards. |
| F5.3 | The inquiry system will be based on one set of Web service security standards that will be used by all carriers. |
| F5.4 | Carriers will develop an inquiry system based on one set of authentication standards. |
| B6 | Verification of evidence of insurance will be sent back to requesting party for appropriate action. |

| Functional and Technical Requirements | |
|---|---|
| **ID #** | **Description** |
| F6.1 | The system will provide a limited verification response: "***Confirmed" or "Unconfirmed***." |
| F6.2 | The system may provide reason codes for unconfirmed results. |
| F6.3 | If the system cannot verify evidence of insurance, it is assumed that the state will rely on its current procedures for insurance verification. |

## Data Dictionary

| Attributes | Data Type | Constraints |
|---|---|---|
| Policy Key | String | Primary Key or Unique Key |
| VIN | String | Primary Key or Unique Key |
| NAIC | String | Unique Key |
| Requested Date | Date | |

| Attributes | Data Type | Constraints |
|---|---|---|
| Tracking Number | String | Primary Key or Unique Key |
| Drivers License Number | String | Primary Key or Unique Key |
| Street Address 1 | String | |
| Street Address 2 | String | |
| City | String | |
| State | String | |
| ZIP | String | |
| Vehicle Make | String | |
| Vehicle Model | String | |
| Vehicle Year | Number | |
| FEIN | String | |

Complete reference documentation that describes the relationships of all data elements contained in the online insurance verification messages can be obtained by contacting the Accredited Standards Committee (ASC) X12 at http://www.x12.org/.

## Technical Specifications

This section describes the technical processes that must be considered if an authorized requesting party wishes to submit a verification request to an insurance carrier's Web service application. It explains the responsibilities of both parties as well as implementation considerations. These processes and considerations are based on the business and functional requirements identified in this guide. The chart below outlines the technical specifications identified by the IICMVA Web Services Tech Team:

| Technical Specifications | |
|---|---|
| **ID #** | **Description** |
| **1** | **Each insurance company will be responsible for the data necessary to verify insurance on their own customers.** |

| Technical Specifications | |
|---|---|
| **ID #** | **Description** |
| 1.1 | Each company will maintain its own data. |
| 1.2 | This data must be accessible by the insurance verification Web service. |
| **2** | **Each insurance company will be responsible for maintaining a Web service through which online insurance verification can take place.** |
| 2.1 | This Web service will provide a Standard External interface. |
| 2.1.1 | This Web service will use SOAP 1.1 message structure. |
| 2.1.2 | Each insurance company will be responsible for publishing a WSDL. |
| 2.1.3 | WSDLs will be published and accessible via a private registry. |
| **3** | **The Web service must be secure.** |
| 3.1 | The message must be authenticated. |
| 3.1.1 | The message will leverage the WS-Security 1.0 specification to authenticate the message. |
| 3.1.2 | The message will be compliant with the WS-I Basic Security Profile 1.0 for interoperability. |
| 3.2 | The message must be secure during transportation. |
| 3.2.1 | The message transport will be encrypted using SSL 3.0 with a 128 bit key. |
| 3.3 | The system will use HTTP 1.1[3] |
| **4** | **It will be the responsibility of the requesting party to determine the appropriate company to which its sends the request.** |
| 4.1 | The endpoint will be determined through use of the NAIC identifier as a routing key. |
| **5** | **The Web service will use a standard XML schema.** |
| 5.1 | This schema will be owned by a standards organization. |
| 5.2 | The standard must be open. |
| 5.3 | The standard must use an open process. |
| 5.3.1 | The standard must be open during development. |
| 5.3.2 | The standard must be open during ongoing maintenance. |

[3] Older versions of network hardware and load balancing equipment may experience difficulties with HTTP 1.1.

| Technical Specifications | |
|---|---|
| **ID #** | **Description** |
| **6** | **Maintain multiple environments** |
| **6.1** | All jurisdictions and carriers must maintain a minimum of two identical environments (one test and one production). |

## Insurance Company Responsibilities

The business and technical specifications require each participating insurance carrier to develop an insurance verification 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 auto insurance company must design, develop, and maintain a Web service capable of verifying the status of a policyholder's insurance information. Each insurance company's Web service ***must*** have a common, or standard, external interface. Standard interfaces are crucial because they allow the requesting party to submit a standard request to each insurance company, reducing the time and cost of maintenance.

Web services developed by insurance companies 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 insurance companies to create a standard external interface. Such a common interface allows each requesting party 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 carrier's WSDL should look similar.

If an insurance company changes the location of its Web service, it is the company's responsibility to provide all necessary requesting parties with the updated endpoint.

The following is a portion of a sample WSDL file:

```
<s:element name="VerifyInsurance2">
        <s:complexType>
                <s:sequence>
                        <s:element name="VINNumber" type="s:int" />
                        <s:element name="strInsuranceCompany" type="s:string" />
                </s:sequence>
        </s:complexType>
</s:element>
<s:element name="VerifyInsurance2Response">
        <s:complexType>
                <s:sequence>
                        <s:element name="VerifyInsurance2Result" type="s:string" />
                </s:sequence>
        </s:complexType>
</s:element>
<service name="Service1">
        <port name="Service1Soap" binding="s0:Service1Soap">
        <soap:address location="http://inscompany.com/verify/VerifyInsurance.asmx" />
        </port>
</service>
```

Although the endpoint is specified in the sample WSDL file, the requesting party will actually retrieve the endpoint for the appropriate insurance company 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 an insurance company's technical infrastructure and data is a primary concern. Therefore, appropriate measures must be taken to prevent unauthorized requesting parties from accessing a policyholder'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.

IICMVA has carefully reviewed two authentication methods to secure the message and the means by which it travels through the Internet. The first, Transport Level Security or Secure Sockets Layer (SSL), uses certificates to prove the identity of the server and/or client. The second, Web Service Security (WS-Security), provides authentication and integrity at the message level.

SSL is a point-to-point solution. Meaning, where the requesting party uses the services of a third party agent or vendor, the insurance company would only be able to verify with certainty that the third party is the caller of its Web service. On the other hand, message level security covers the scope of the entire request. While message layer authentication has its benefits, there are implementation complexities that come with it. SSL with client authentication provides a very secure and reliable means of authentication and protection of data; therefore, the IICMVA recommends the use of SSL with client authentication.

### *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 insurance company. In turn, SSL 3.0 with client authentication allows an insurance company 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.

Mutual SSL is discretionary. Meaning, insurance companies that wish to use SSL can do so, and insurance companies that do not wish to exchange certificates can simply ignore the client certificate.

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

### *Message Level Security*

For Message Level Security, insurance companies will use the ***WS-Security specification protocol*** and will need to support multiple authentication token types. Ideally, the same X.509 certificate sent for Mutual SSL could be sent in the SOAP header for message level authentication. If not, a username and password pair could be used. The message will be compliant with the ***WS-I Basic Security Profile 1.0*** for interoperability.

An authentication token provided in the SOAP header using WS-Security would look similar to the following example:

```
<soap:Header>
…
        <wsse: UsernameToken xmlns:wsu="http://docs.oasis-
                open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
                1.0.xsd" wsu:Id="SecurityToken-02cf5c9c-8635-4ac5-b77a-
                666521bc6dff">
                        <wsse: Username>Tester</wsse:Username>
                        <wsse: Password Type="http://docs.oasis-
                                open.org/wss/2004/01/oasis-200401-wss-username-token-
                                profile-1.0#PasswordText">testPassword@1</wsse:Password>
                        <wsse:Nonce>x/8L/bSduwsMdYmi+cP9iw==</wsse:Nonce>
                        <wsu:Created>2004-10-06T19:33:47Z</wsu:Created>
        </wsse:UsernameToken>
…
</soap:Header>
```

### *Maximum Participation*

The use of both authentication methods allows for maximum participation by insurance carriers, regardless of their present infrastructure. States must support both methods to permit all carriers to participate.

Although a transport authentication session by itself provides adequate security levels, the additional message level authentication satisfies the security standards within the IT shops of many large insurance carriers. Additional flexibility is made available by allowing carriers the option to use transport authentication by itself if they are not equipped with the necessary resources to handle message level authentication. On the contrary, carriers could use message only security if that satisfies their requirements.

## Authorized Requesting Party Responsibility

Each authorized requesting party or state is responsible for developing an insurance verification ***Web service client*** based on the standards identified in Section 4 above. The following information explains the technical specifications behind this requirement in more detail:

### Collect the Key Information Needed to Submit an Inquiry

Each authorized requesting party must determine how it will collect the basic information needed to submit a standardized inquiry request.

### Build and Maintain a Web Service Client

The authorized requesting party must develop a Web service client capable of sending a request to an insurance carrier's Web service. Each requesting party's Web service client must provide the required information necessary to invoke a request and verify a policyholder's insurance information.

The Web services developed by the insurance companies will adhere to the SOAP 1.1 standards. Therefore, the requesting 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, the requesting parties 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, the requesting parties will need to store an endpoint indicating the location of each carrier'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 carrier. However, due to the risk of exposing each insurance company's service endpoint, IICMVA recommends that each state host its own Web service client and manage all endpoints for their particular state.

### Route the Request to the Appropriate Insurance Carrier

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 requesting party's application should contain logic that correlates an insurance company's name or National Association of Insurance Commissioners (NAIC) code with the appropriate endpoint record.

### Maintain and Store Access Credentials

Since the insurance verification 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 the insurance companies with a renewed certificate 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.

## Implementation Scenarios for Authorized Requesting Parties

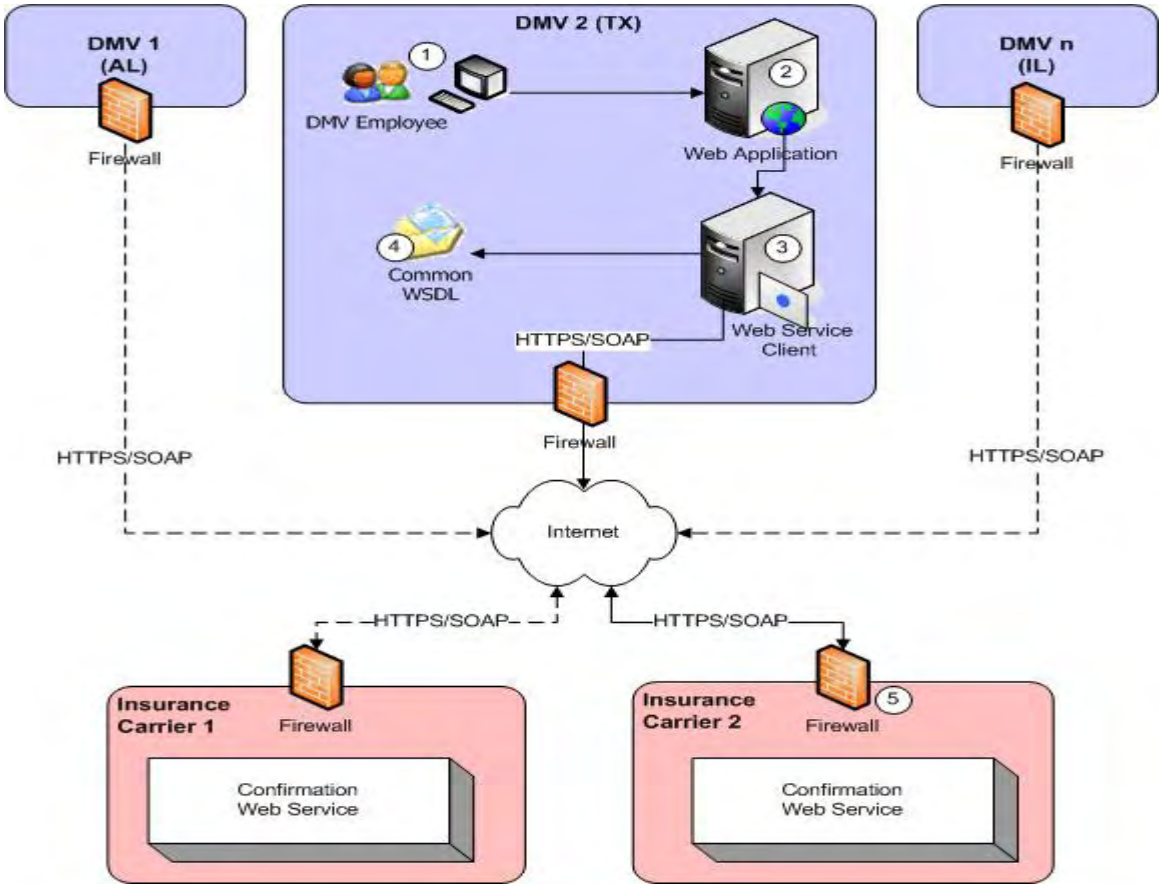
The following diagrams have been provided to illustrate the different possibilities that exist when a requesting party implements a Web service client using internal resources or a third party vendor.

The use of a vehicle registration scenario does not imply the only application for the insurance verification Web service application.

According to software engineering best practices and technical requirements 6 and 6.1 there is a need for all parties to implement at least 2 environments (at least one for testing and one for production) regardless of the implementation scenario selected. Only one scenario should be selected and implemented for all environments by each participating party.

### Implementation Scenario #1: No Third Party Intermediary

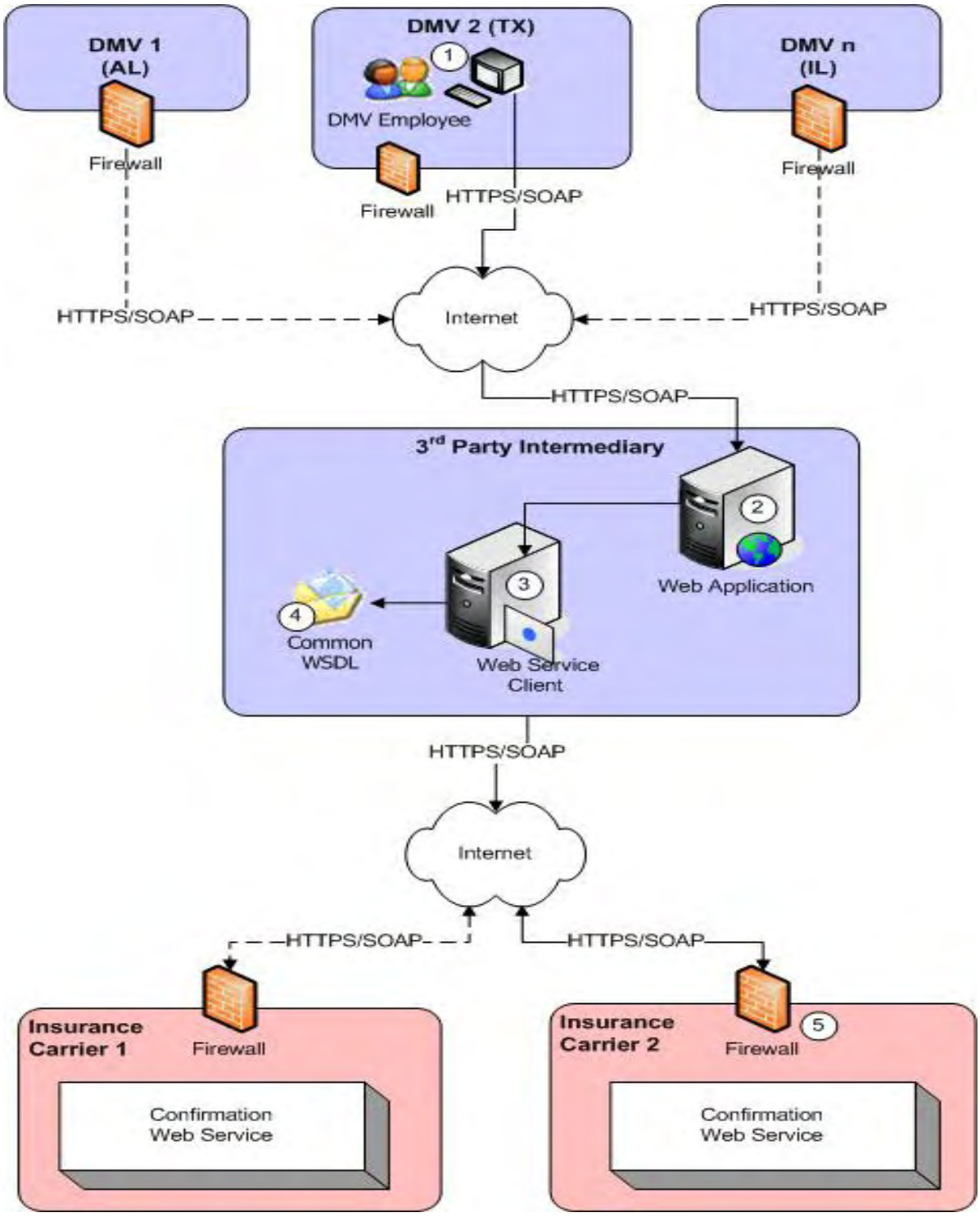
In this scenario, the requesting party requests verification of evidence of insurance from an insurance carrier. The request is fully automated and enabled by Web services. The verification request is exchanged directly between a State DMV (authorized requesting party) and an insurance carrier.




1. During the license plate registration process, an automobile owner provides insurance carrier information about the vehicle being registered. The clerk then enters the policy holder's information into their system.
2. In this scenario, the Web application is located and maintained at the DMV. This is the application used by the DMV clerk in step 1.
3. There is a logical separation between the Web application and the Web service. Although not required, the Web application and Web service can be located on separate physical servers if desired.
4. Since each carrier's Web service interface will be the same, it is only necessary for the DMV to maintain a single WSDL file. This will likely be located on the same server as the Web service.
5. The insurance carrier's Web service will receive the request, perform the backend transactions necessary to determine whether a motorist is insured, then return the confirmation to the DMV.

### Implementation Scenario #2: Third Party Intermediary

In this scenario, the authorized requesting party requests the verification of evidence of insurance from an insurance carrier through a third party intermediary or vendor. The intermediary third party provides a Web service transaction routing service.



1. During the license plate registration process, an automobile owner provides insurance carrier information about the vehicle being registered. The clerk then enters the policy holder's information into their system.
2. In this scenario, the Web application is located and maintained by a 3rd party agent chosen by the DMV. This application is used by the DMV clerk in step 1.
3. There is a logical separation between the Web application and the Web service. Although not required, the Web application and Web service can be located on separate physical servers if desired.
4. Again, since each carrier's Web service interface will be the same, it is only necessary for the DMV to maintain a single WSDL file. This will likely be located on the same server as the Web service.
5. The insurance carrier's Web service will receive the request, perform the backend transactions necessary to determine whether a motorist is insured, then return the response to the DMV.

## XML Payload Message

XML messages for online insurance verification have been independently developed by the ***American National Standards Institute (ANSI)*** and the ***Association for Cooperative Operations Research and Development (ACORD).***

At this time, both standards bodies have not developed one unified XML schema that IICMVA can reference in this guide.

## Service Level Agreements (SLA) and Volume Metrics

It will be the responsibility of the participating insurance companies to abide by the Service Level Agreement (SLA) established with the requesting party. Each company will have different business volume metrics; therefore, each carrier will need to build an infrastructure that allows for compliance with the established SLA.

The Service Level Agreement is composed of a minimum of 4 areas:

### Response Time

Response time is the total time elapsed from when a request is initiated to the time the response is received and is made available to the requesting party.

For the state, response time is a key factor in determining the success or failure of an inquiry and the overall success of the service. The state must determine acceptable response time(s) taking into account the components described below that contribute to the overall measurable response time and determining what is acceptable based on the needs of the user. A response received within the time threshold established by the state is considered a successful transaction; a response received outside of the established time threshold is deemed a failed transaction. For failed transactions, the state would further establish a protocol or procedure to address failed transactions. Such procedures may include, but not limited to, if and when to re-initiate the inquiry (immediately or at some time in the future), monitoring success/failure rates and examination of the service components when response time exceeds tolerances.

Several components make up this total measurable response time and understanding each component and how it may affect user perceived response time is important when establishing service level agreements (SLA's) related to response time.


Total response time is affected by (at least) three (3) possible measurements:

| Component | What can be Measured |
|---|---|
| State sends request to Vendor contracted by the state, the Insurance Carrier, or the Insurance Carrier's Web Services provider | Response time may be measured from the time the State initiates the Request until the time the state receives the Response. |
| Vendor sends request to Insurance Carrier<br>or<br>Vendor sends response to State | Response time may be measured from the time the request or response reaches the Vendor's firewall to the time the request or response leaves their firewall. |
| Insurance Carrier (or Web Services provider) sends response to Vendor or State | Response time may be measured from the time the request reaches the Insurer's (or Web Services provider's) firewall to the time the response leaves their firewall. |

**Note:** The above measurements do not make reference to the unknown time (Internet) which is outside of the firewall.

As an insurance industry we strive to achieve the best possible response time for state on-line verification (OLV) requests. Based on average historical data received from current OLV states the median response time is approximately five (5) seconds.

Contributing factors that may affect OLV response time that should be taken into account:

- Broadband/WAN issues
- Internet traffic and time of day
- Time outs – due to internet broadband issues
- Submission failures due to web service limitations
- Increased service volume due to additional authorized requestors

As states move to an OLV program, insurance carriers will need to monitor and make the necessary server capacity adjustments to mitigate any impact to OLV response time.

### Historical Verification of Evidence of Insurance

The IICMVA recommends that insurance carriers should maintain up to six (6) months worth of evidence of vehicle insurance data from the current date if the state is planning to use the OLV process.

### System Availability

Each insurance carrier shall assume the responsibility to provide an online system able to respond to verification requests on an on-demand basis with high availability. As with all systems, a reasonable amount of down time is expected to maintain carrier systems, commonly referred to as "planned system outages".

IICMVA recommends maintaining a list of technical contacts that are available to regulatory agencies to assist with any problems or unplanned system outages.

### Testing Period

An appropriate amount of lead time for implementation and testing should be provided in advance of implementation of the verification program. IICMVA recommends a testing period of no less than (nine) 9 months be established to provide that insurance carriers and jurisdictions can ensure a fully functional verification program.

## Impact of Batch Requests

Web services are built for online, instant requests and responses. Like a telephone conversation, a requesting party stays connected to a Web service until the application completes the request, usually within seconds. This is called a ***synchronous request.***

If a requesting party submits a request that cannot be fulfilled by the application service during the initial network connection, an ***asynchronous request*** has been initiated. Essentially the phone conversation ends and the Web service application has to call the requesting party back at another time to fulfill the service.

Since the structure of a Web service call is XML, it would be relatively easy to receive multiple verification requests within one Web service call via a batch request. However, there are multiple impacts, including delayed response time and additional infrastructure requirements.

The structure of the request is very flexible because it is string-based and all applications can parse and process the string data structure. The downside, however, is that the structure can produce a significant amount of overhead.

For example, to verify a motorist is currently insured, part of the message may look like the following XML structure:

```
<Motorists>
    <Motorist>
        <PolicyNumber></PolicyNumber>
        <VIN></VIN>
        <NAIC></NAIC>
        <ConfirmationDate></ConfirmationDate>
        <RefNumber></RefNumber>
        <LicenseNumber></LicenseNumber>
        <InsuredName></InsuredName>
        <Address>
            <StreetPOBox></StreetPOBox>
            <City></City>
            <State></State>
            <ZipCode></ZipCode>
        </Address>
        <Vehicle>
            <Make></Make>
            <Model></Model>
            <Year></Year>
        </Vehicle>
        <FEIN></FEIN>
    </Motorist>
</Motorists>
```

This sample XML structure does not include data for each element. However, imagine the example multiplied by 1000. While possible to receive and process, such a request would take a significant

amount of time to handle; therefore, it should be processed during non-peak hours. If the request is received at 1:00 PM and processed at 12:00 AM, an asynchronous request would be established.

Of course, asynchronous processing has a significant impact on the requesting party as well. Instead of simply creating a Web service client to submit requests to insurance carrier Web services, requesting parties would need to develop a Web service to which asynchronous responses could be posted by insurance carriers.

Serious consideration should be given before requesting batch processing via the insurance verification Web service application.

## Implementation Processes and Testing Strategy

To ensure a consistent quality product across carriers 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 Online Insurance Verification

## Test Strategy

### Test Objectives

- Verify that the requesting party is able to send a valid ANSI X12 XML message
- Verify that the receiving party is able to receive and respond with a valid ANSI X12 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.

i. For all levels and types of tests, test cases will require, but not be limited to: VIN, policy number, verification date, and NAIC code.

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 VIN, policy number, evidence of insurance verification date, and NAIC code.

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 state jurisdiction 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 state 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 state jurisdiction to be used for Authentication/Authorization/Accounting.

3. If required, the state 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 insurer shares the IP address and certificate authorities.

5. The state jurisdiction (or its appointed representative) provides insurers with their organization name which is included in the XML message. The insurer includes these details in their database to validate that the state jurisdiction is considered a valid requesting party.

# *APPENDIX B*

## Schema Variations

The most notable variations between the current schema version (September 2008) and prior version of the schema are the expanded Request and Response codes and corresponding code values. While the Request Codes were merely expanded, the Response codes were expanded and given new code values.

## Request Codes

Schema Versions 00200510[4]

| Description | Code Value |
|---|---|
| Bodily Injury (BI) Coverage Verification | BI |
| Personal Injury Protection Coverage (PIP) Verification | PIP |

Schema Version 00200809[5] (Current)

| Description | Code Value |
|---|---|
| Accident | ACC |
| Traffic Violation with Accident | ACCV |
| Bodily Injury (BI) Coverage Verification | BIVER |
| Personal Injury Protection Coverage (PIP) Verification | PIPVER |
| Registration Renewal | REGREN |
| Registration of Vehicle | VEHREG |
| Traffic Violation | VIOL |

[4] Accredited Standards Committee X12, Insurance Subcommittee, ASC X12N. "Requests Codes" Coverage Request V00200110. < http://xml.x12.org >.

[5] Accredited Standards Committee X12, Insurance Subcommittee, ASC X12N. "Requests Codes" Coverage Request V00200809. < http://xml.x12.org >.

## Response Codes

Schema Versions 00200510[6]

| Description | Code Value |
|---|---|
| Incorrect Data Format | 1 |
| Missing Unique Key | 2 |
| Missing NAIC Code | 3 |
| Missing VIN | 4 |
| Missing Verification Date | 5 |
| Unauthorized Requestor | 6 |
| System Cannot Locate Unique Key – Information | 7 |
| System Found Unique Key – No coverage on Date Requested | 8 |
| System Found Unique Key – VIN Cannot Be Verified | 9 |
| System Found VIN – Unique Key Cannot Be Verified | 10 |
| System Cannot Locate Policy Information – Manual Search In Progress | 11 |
| System Unavailable | 12 |

Schema Version 00200809[7] (Current)

| Description | Code Value |
|---|---|
| Incorrect Data Format | IDF |
| NAIC Code Not Submitted | NAIC1 |
| System Cannot Locate NAIC | NAIC2 |
| Policy Key Not Submitted | PKEY1 |
| System Cannot Locate Policy Key Information | PKEY2 |
| System Found Policy Key – Coverage on Verification Date Cannot Be Confirmed | PKEY3 |
| System Found Policy Key – VIN Cannot Be Verified | PKEY4 |
| System Cannot Locate Policy Information - Manual Search in Progress | POL1 |
| System Unavailable | SYSU |
| Unauthorized Requestor | UREQ |
| Coverage on Verification Date Cannot Be Confirmed | VDT1 |
| Verification Date Not Submitted | VDT2 |
| System Cannot Locate VIN | VIN1 |
| System Found VIN – Coverage on Verification Date Cannot Be Confirmed | VIN2 |
| System Found VIN – Policy Key Cannot Be Verified | VIN3 |
| VIN Not Submitted | VIN4 |

| | |
|---|---|
| | Codes and descriptions that **would** be used when responding if the requesting party failed to provide data for mandatory elements. |
| | Codes and descriptions that **could** be used after processing the request which resulted in an unconfirmed response. |
| | Code and description indicating that some technical problem caused the system to be unable to return a response. |

[6] Accredited Standards Committee X12, Insurance Subcommittee, ASC X12N. "Requests Codes" Coverage Response V00200510. < http://xml.x12.org >.

[7] Accredited Standards Committee X12, Insurance Subcommittee, ASC X12N. "Requests Codes" Coverage Response V00200809. < http://xml.x12.org >.

## 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 verification, 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 verification have been independently developed by the ***American National Standards Institute (ANSI)*** 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

- ***Requesting Party*** can be a State 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 companies. ***Authentication*** is the process of verifying the identity of a person or entity. For online insurance verification, 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*

8/15/2005 has been revised to clarify the data elements used to initiate a verification request.

Several DMV administrators indicated that some terms and concepts were unclear during a user guide walkthrough held at the headquarters of the American Association of Motor Vehicle Administrators (AAMVA) in Arlington, Virginia, on September 19-20, 2005:

2.0 The phrase "***Online Status"*** in the *Executive Summary* has been clarified with more detail.

3.0 An explanation has been provided in the *User Guide Purpose* section regarding why DMVs are the only ***authorized requesting parties*** recognized by insurers providing this online service.

4.0 The data element "***Unique Key/Policy Number***" has been changed to the term "***Policy Key"*** since it truly reflects the use of policy numbers or policy number references used by carriers to locate specific policy records in their individual internal databases.

5.0 The meaning of **UNCONFIRMED** has been clarified in the *System Distributes Communication* section.

6.0 A comment is provided in the *System Distributes Communication* section to state that financial responsibility limits are not returned to the requesting party.

- Reason codes for **UNCONFIRMED** results have been eliminated and replaced with a reference to the available XML standards bodies that have developed messages for the online auto insurance verification application.
- The term "***minimum financial responsibility coverage***" has been substituted for "***auto liability limits***" or similar references to be more inclusive of states that have alternative requirements in addition to auto liability insurance coverage.
- The document has been separated into sections separating business requirements from the technical requirements and implementation recommendations.

## 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.