

Model User Guide for Implementing Online Insurance Verification

Using Web Services to verify evidence of auto liability insurance

*Version 7.0
January, 2017*



*Insurance Industry Committee on
Motor Vehicle Administration*



Executive Summary

Mandatory liability insurance laws exist in 49 states and the District of Columbia. Auto Liability Insurance Reporting (ALIR) programs, often referred to as state reporting systems and implemented in a majority of states, are designed to enforce compulsory insurance by providing jurisdictions with the means to identify uninsured motorists.

Evidence strongly suggests, however, that these programs are failing to achieve this objective. In addition to not performing as expected, state reporting systems are costly, difficult to implement, hard to maintain and a financial burden for insured drivers (who must pay for the costs of such programs through higher premiums).

Recent and ongoing advances in technology, such as web services and internet-based transaction processing, however, substantially improve the effectiveness of ALIR programs by providing for online verification of evidence of auto insurance. Accordingly, the Insurance Industry Committee on Motor Vehicle Administration (IICMVA) strongly recommends the use of web services technology as outlined within this guide for the purposes of verifying evidence of auto insurance.

Forward

About the IICMVA

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

Ad hoc committees are necessarily restrictive and inconsistent in function and composition. IICMVA was formed to provide consistent, industry-wide exchange between the insurance industry and all state jurisdictions.

The IICMVA's basic organization is built around insurers and insurance trade associations. The three major insurance trade associations are the 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). Non-affiliated insurers round out the IICMVA roster.

The 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 (AAMVA).

Business Direction

Technology has evolved significantly since the late 1950's when states first began enforcing 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 continue to 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

The IICMVA views this technology as the most effective and efficient way to resolve what has become a controversial public policy issue: enforcement of mandatory or compulsory insurance laws.

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

Enforcement of mandatory or compulsory insurance laws through the use of web services 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 would soon be a reality in the realm of insurance verification.¹ It behooves the insurance industry to seize this opportunity to advance the effectiveness of insurance verification programs.

Vision

The Committee strongly supports an event-based, online inquiry approach to the verification of evidence of insurance. The model outlined within this guide reflects this approach.

IICMVA's vision includes simple online applications that support single policy inquiries. This vision incorporates the use of true web services that support the interconnection of systems between authorized trading partners, namely insurance companies 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 company'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 company's IT environment.
- The matching limitations and data integrity issues of current state reporting programs are eliminated.
- Customer service is improved because primary search criteria are based on the business rules within each company.
- Commercial insurance companies are in a better position to comply with state mandates.
- Insurance companies 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.
- Privacy is protected: Only designated, legally authorized entities will have access. The information provided is limited and state of the art technological safeguards, such as the latest methods of encryption, are included.

All of these benefits combine to render web service technology the most effective and accurate method of verifying evidence of financial responsibility currently available.

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

Table of Contents

Section One.....	3
Introduction to the Model User Guide	3
Program Goals	3
Program Purpose	3
User Guide Purpose.....	3
Program Overview	3
Program Process Overview	4
Authorized Requesting Party Submits Evidence of Insurance Verification Request	4
System Validates Request.....	5
System Determines Verification Result	5
System Distributes Communication	5
Unknown Carrier Response Communication.....	6
Program Process Requirements	6
Business Requirements	6
 Section Two.....	 7
Technical Processes and Considerations	7
Technical Overview.....	7
Web Services.....	7
Open Standards	7
Internet.....	7
Security	8
Functional and Technical Requirements	8
Technical Specifications	12
Insurance Company Responsibilities	13
Build and Maintain a Web Service and Common External Interface.....	13
Distribute the WSDL File Accordingly.....	14
Manage One Common WSDL File.....	14
Secure the Web Service	14
Transport Level Security	15
Authorized Requesting Party Responsibility.....	15
Collect the Key Information Needed to Submit an Inquiry	15
Build and Maintain a Web Service Client	15
Route the Request to the Appropriate Insurance Company	16
Maintain and Store Access Credentials	16
Implementation Scenarios for Authorized Requesting Parties.....	17
Implementation Scenario #1: No Third Party Intermediary	17
Implementation Scenario #2: Third Party Intermediary	18
XML Payload Message.....	19
Service Level Agreements (SLA) and Volume Metrics.....	19
Response Time.....	19
System Availability	20
Testing Period.....	20
Historical Verification of Evidence of Insurance	20
Impact of Batch Requests.....	20
Implementation Processes and Testing Strategy.....	22

APPENDIX A.....	23
Implementation Processes and Testing Strategy for Online Insurance Verification.....	23
Test Strategy.....	23
Setup Checklist.....	23
APPENDIX B.....	24
Schema Variations	24
Request Codes	24
APPENDIX C	26
Business Rules.....	26
Request and Response Data Elements.....	26
Request Data Elements.....	27
Response Data Elements	29
GLOSSARY.....	31
SUMMARY OF REVISIONS	33
BIBLIOGRAPHY.....	34

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 jurisdictions.
- Improving data security by eliminating the transfer of detailed policy information.

Program Purpose

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

Other insurance verification models require insurance companies to report insurance policy information which is then compared to vehicle registration data maintained by motor vehicle departments. Under this model, any vehicle registrations not tied to an insurance record are considered uninsured. Unfortunately, data integrity problems inherent to this type of verification process render it an inaccurate method of verifying evidence of insurance. Repeated exchanges of data between insurance companies 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 a model requiring insurance policy data reporting: ***online insurance verification or inquiry via web services.***

By utilizing the online insurance inquiry model, evidence of financial responsibility may be verified at the occurrence of a financial responsibility event.

Online verification eliminates the need to match insurance company 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 authorized entities, such as Departments of Motor Vehicles, to go directly to the source of insurance information – the insurance companies themselves.

User Guide Purpose

The purpose of this guide is to provide insurance companies and state jurisdictions (or their agents) with the information needed to verify evidence of auto financial responsibility via web service applications.

This guide provides both business and technical information on how **requesting parties** (e.g., Department of Motor Vehicles, Department of Safety or their authorized agent) may submit insurance verification requests to web services hosted by participating insurance companies. Section One focuses on the general business process while Section Two addresses the technical recommendations and elements to be followed by parties implementing this solution.

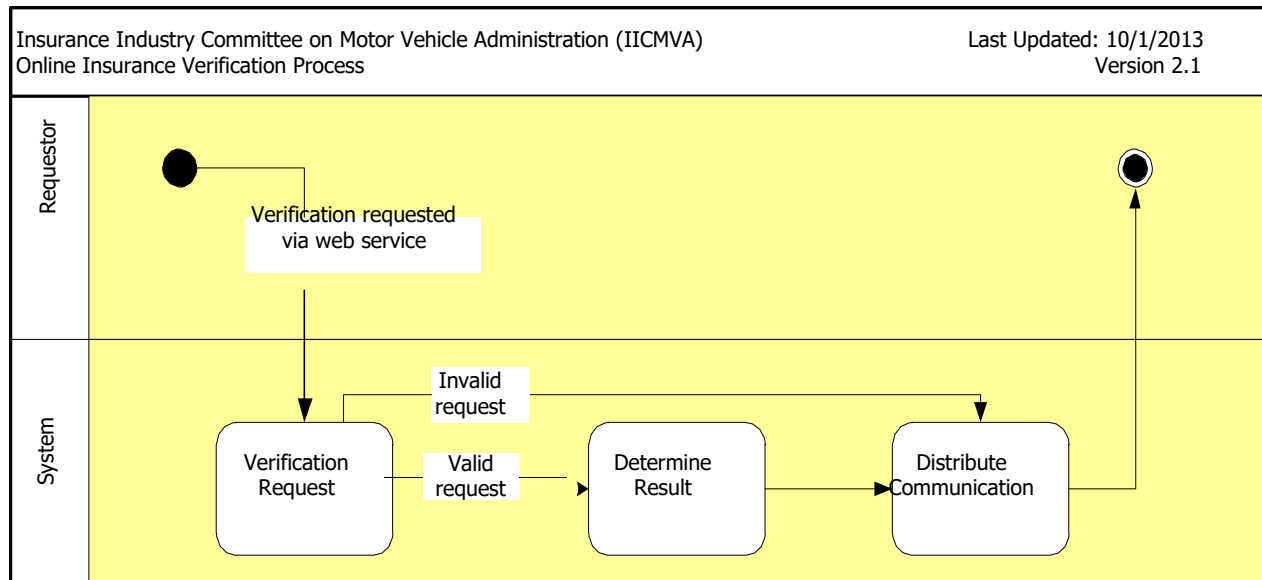
Program Overview

When presented with a financial responsibility event, the requesting party (e.g., Department of Motor Vehicles, Department of Public Safety or their authorized agent) simply submits a standardized ***request for verification of evidence of insurance*** to the web service of a participating insurance company. In turn, the insurance company replies with a standardized ***evidence of***

insurance confirmation (or unconfirmed) 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 financial responsibility on a date in question. *It does not identify the coverage limits of a particular policy or substitute for an insurance company's claims handling function because it is unable to confirm an insurance company'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 company.

The request will be sent in an XML payload message. The message content key from the requesting party shall include **mandatory** data elements; NAIC, Policy Key, VIN and Verification Date (See Functional and Technical Requirements).

Interpretation of the request without the **mandatory** data elements (Functional and Technical Requirements T3.2.3), along with the response being provided is solely the responsibility of the insurance company receiving the request.

The message content key from the requesting party may include **optional** data elements (Functional and Technical Requirements T3.2.4). (Optional data elements may be accepted/provided by the sole discretion of each participating insurance company and this model does not contemplate the mandatory provision of the data elements other than those required.)

In August 2011, the IICMVA modified the model to include the ability of the requester to submit an **unknown request** when the insurance company and/or Policy Key are not known at the time of an event that would trigger a verification request. The value of "UNKNOWN" in the Policy Key field allows the requestor to formulate a valid inquiry which can be sent to an

insurance company (by means of identifying the appropriate NAIC number).

This option may not be available for non-vehicle specific policies, which is the case for many customers provided insurance through a commercial policy.

The results of such an unknown request could be one of several responses which are noted under **System Determines Verification Results** below.

System Validates Request

The web service application of the participating insurance company validates the request meets the following conditions:

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

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

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 *response codes* available from the ASC X12 or ACORD standard specifications.

System Determines Verification Result

The web service application 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 company's database.
- The system determines financial responsibility compliance on the requested verification confirmation date.

System Distributes Communication

For valid evidence of insurance verification requests:

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

An **UNCONFIRMED** result may be an indication of one or more of the following:

- The insurance company could not identify the matching policy information with the input provided;
- Financial responsibility was not confirmed for the verification date requested; and/or

- One or more data elements submitted could not be matched.

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

Proprietary business rules of each insurance company determine whether an **UNCONFIRMED** response is accompanied by reason messages.

***NOTE:** Privacy concerns dictate that detailed policy information is not part of the result due to the use of the public internet. However, the verification result does provide what is most important: verification of financial responsibility. Coverage limits are not provided, as a confirmed response verifies minimum financial responsibility has been met.*

The web service application eliminates 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 company. This allows for a more accurate result.

Unknown Carrier Response Communication

- **VALID REQUEST RESPONSE – CONFIRMED**

Company systems designs that match on VINs only will return a confirmed response.

- **VALID REQUEST RESPONSE - UNCONFIRMED**

Insurance companies may accept the unknown request; however, the response will not be confirmed without the policy key matching a key in their system. These companies may provide a response code with the unconfirmed response, depending on their individual business and legal requirements. The response code would also be dependent upon the XML schema version in use by the insurance company ([Appendix B](#) – Schema Versions).

- **REJECTED - INVALID REQUEST**

Companies which developed their web service based on a previous version may not recognize "UNKNOWN" as a data element.

***NOTE:** Versions evolve over time due to changing business requirements and the requirements of the national standards development organizations. Please refer to the ASC X12 and ACORD standards organizations' web sites (www.ASCX12.com and www.ACORD.com) for the most up-to-date national standardized protocols. See Appendix B for request and response codes and corresponding values at the time of this writing.*

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>. This publication was revised in 2010 and is now entitled ***Making the Case for Using Web Services to Verify Evidence of Auto Liability Insurance:*** <http://www.iicmva.com/White%20Paper%202.0.pdf>.

The following business requirements are traceable to the technical specifications outlined in Section Two of this guide. These requirements are complimented by the functional 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 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 inquiries will be made using key information to route a request to the appropriate insurance company for a response.
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.
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 transmitted to the requesting party.

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 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 companies 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 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 (WSI)
- 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 insurance companies 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 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.
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 financial responsibility.
T2.1.1	The system will be built on an infrastructure (i.e.; <i>how</i> 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: <i>This is not a batch processing requirement.</i>)
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 insurance company for a response.
F3.1	Insurance companies will individually decide at what level they will verify evidence of insurance to a requesting party: <i>policy level</i> or <i>vehicle level</i> .

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	<p>The message content key from the requesting party will include the following mandatory data elements:</p> <ul style="list-style-type: none"> Policy Key <p><i>The Policy Key for each insurance company may be a company's policy number, or a number that a company uses internally to locate a policy record.</i></p> <p><i>If a jurisdiction wishes to send a verification request for a specific vehicle but the insurance company and/or Policy Key is unknown, an unknown request can be sent to any insurance company. To accomplish this, a value of "UNKNOWN" should be placed in the Policy Key field.</i></p> <p>Note: <i>This option may not be available for non-vehicle specific policies, which is the case for many commercially insured customers.</i></p> Vehicle Identification Number (VIN) <p>Note: <i>VIN is used by insurance companies that will verify evidence of insurance at the vehicle level. Some companies may choose to confirm insurance at the policy level.</i></p> NAIC (National Association of Insurance Commissioners) Code Requested Verification Date

Functional and Technical Requirements	
ID #	Description
T3.2.4	<p>The message content key from the requesting entity may include the following optional data elements:</p> <ul style="list-style-type: none"> Tracking / Reference Number <p>Note: <i>The system shall provide the ability to accept and return a reference number so that an authorized requester can tie together a verification request with a verification response.</i></p> Drivers' License Number Named Insured Name Address: <ol style="list-style-type: none"> Street/PO Box City State Zip Vehicle Make Vehicle Model Vehicle Year Federal Employer Identification Number (FEIN)
B4	The information exchanged will be limited to only those items needed to accurately route the request and response messages, thus minimizing privacy concerns.
F4.1	A legal trading partner agreement between insurance companies 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 insurance companies.
F5.4	Insurance Companies will develop an inquiry system based on one set of authentication standards.

Functional and Technical Requirements	
ID #	Description
B6	Result Confirmation of evidence of insurance inquiry will be transmitted to the requesting party for appropriate action.
F6.1	The system will provide a limited verification response: "Confirmed" or "Unconfirmed."
F6.2	The system may provide response 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.

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 company'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.

Technical Specifications	
ID #	Description
1	Each insurance company will be responsible for the data necessary to verify evidence of insurance.
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 it 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.
6	Maintain multiple environments
6.1	All jurisdictions and insurance companies must maintain a minimum of two identical environments (one test and one production).

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

Insurance Company Responsibilities

The business and technical specifications require each participating insurance company 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 insurance company'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:elementname="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.

Transport Level Security

For Transport Level Security, insurance companies will use TLS 1.2 for transport level security. TLS1.2 enables requesting parties to know they are communicating with the correct insurance company. In turn, TLS 1.2 with client authentication allows an insurance company to know it is communicating with the correct authorized party.

TLS 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.

TLS 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.

The following table represents some commonly trusted, but not all inclusive, certificate authorities.

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

Authorized Requesting Party Responsibility

Each authorized requesting party or state is responsible for developing an insurance verification ***web service client***. 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 company'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 insurance company'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 company. However, due to the risk of exposing each insurance company's service endpoint, the 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 Company

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 two 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

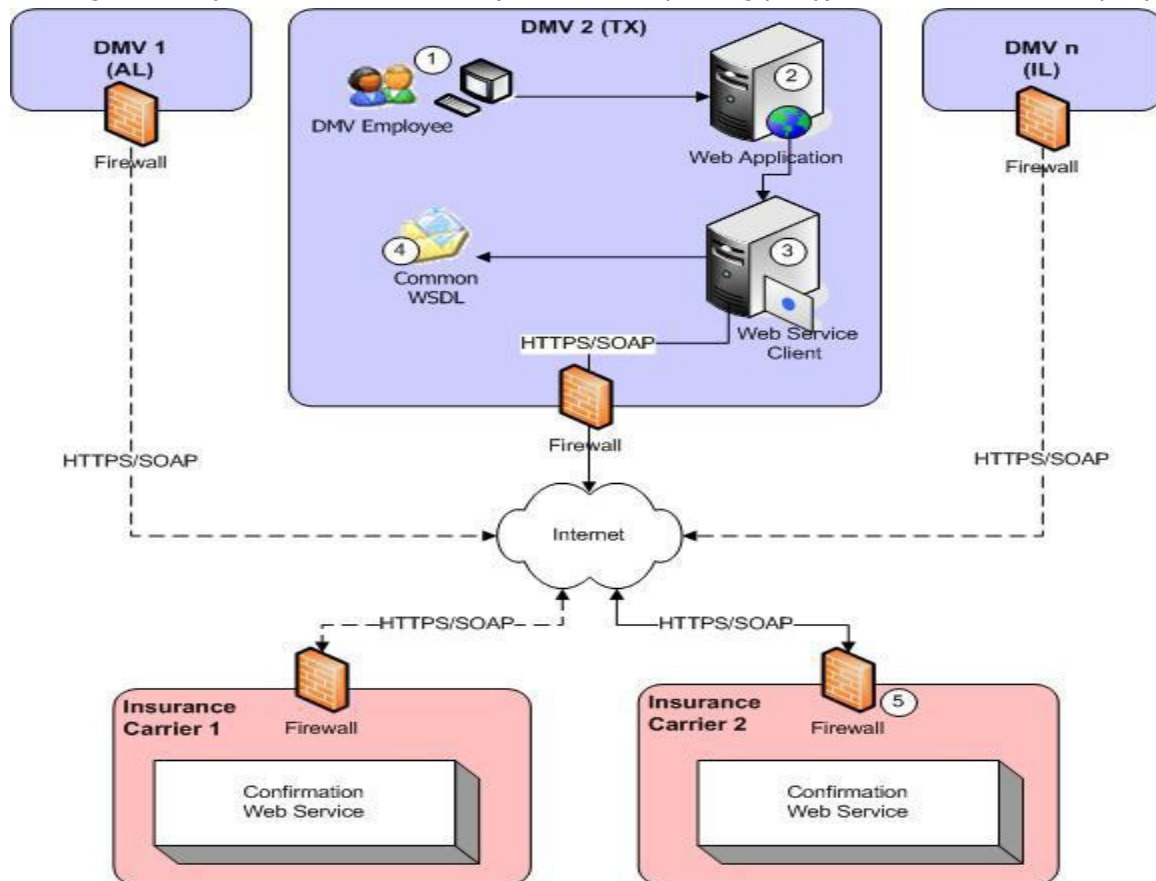
The following diagrams have been provided to illustrate the different possibilities that exist when a

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 two 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 company. 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 company.

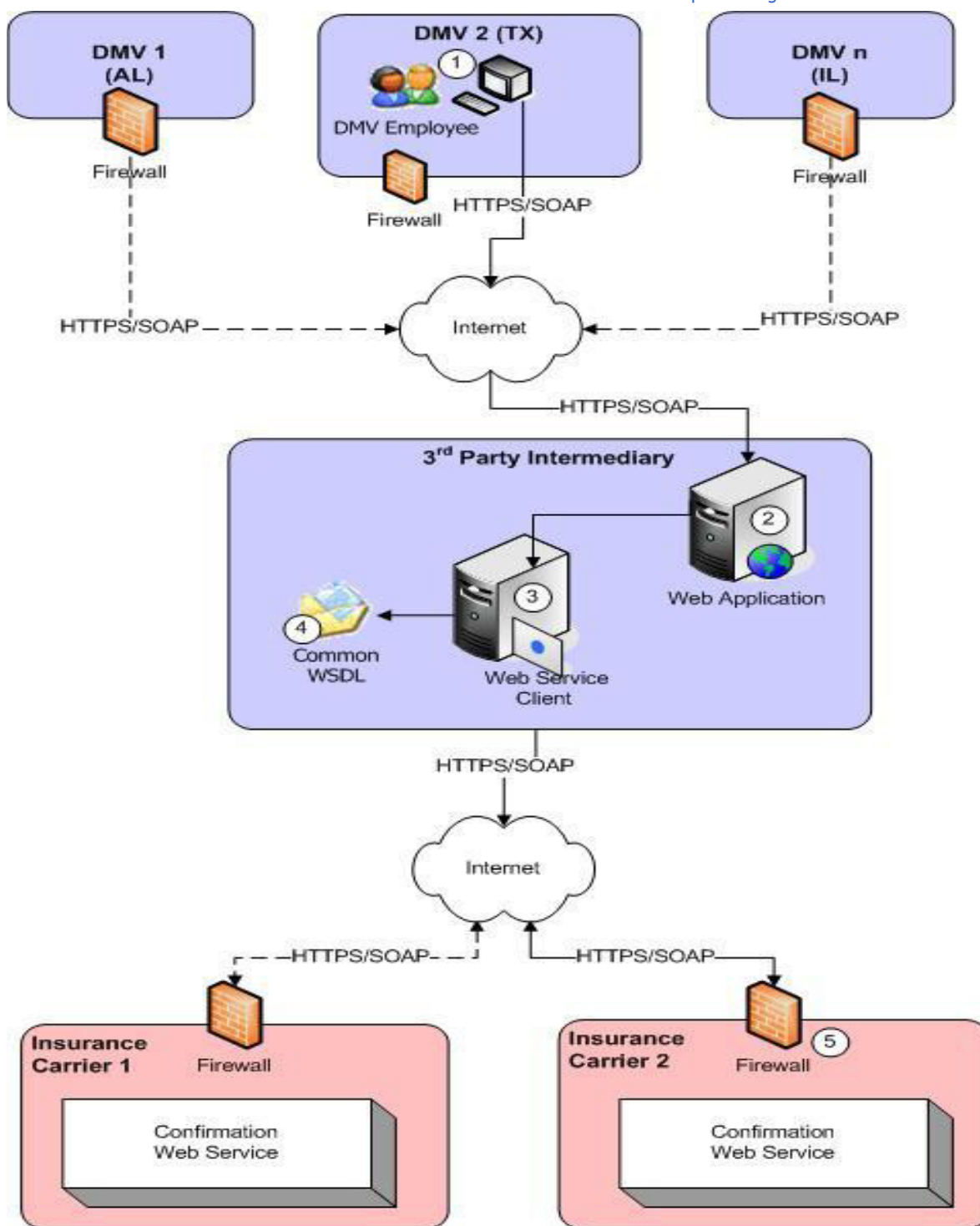


1. During the license plate registration process, an automobile owner provides insurance company information about the vehicle being registered. The clerk then enters the policyholder's information into their system.
2. In this scenario, the web application is located and maintained at the DMV. This 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 insurance company'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 company's web service will receive the request, perform the back-end transactions necessary to determine whether evidence of insurance exists for the vehicle or policy in question, and then return the response message 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 company 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 company information about the vehicle being registered. The clerk then enters the policyholder's information into their system.
2. In this scenario, the web application is located and maintained by a third-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 insurance company'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 company's web service will receive the request, perform the back-end transactions necessary to determine whether evidence of insurance exists for the vehicle or policy in question, and then return the response message to the DMV.

XML Payload Message

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

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 insurance company will need to build an infrastructure that allows for compliance with the established SLA. The Service Level Agreement is composed of a minimum of four 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 reinitiate 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 Company, or the Insurance Company'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 Company or 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 Company (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 companies will need to monitor and make the necessary server capacity adjustments to mitigate any impact to OLV response time.

System Availability

Each insurance company 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 company 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 companies and jurisdictions can ensure a fully functional verification program.

Historical Verification of Evidence of Insurance

Insurance companies will respond to a request with a verification date up to six months prior to the current date. Any requests with a verification date more than 6 months prior to the time the request is made may not produce desired results.

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 company web services, requesting parties would need to develop a web service to which asynchronous responses could be posted by insurance companies. *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 insurance 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 Online Insurance Verification

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. Receiving party returns the response XML message 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

ASC X12 Schema Version 00200510⁴

Description
Accident
Traffic Violation with Accident
Coverage Verification
Registration Renewal
Registration of Vehicle
Traffic Violation

ASC X12 Schema Version 00200809⁵

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

⁴ Accredited Standards Committee X12, Insurance Subcommittee, ASC X12N. "Request Codes" Coverage Request V00200510. < <http://xml.x12.org> >.

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

Response Codes

ASC X12 Schema Version 00200510⁶

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

ASC X12 Schema Version 00200809⁷ (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> >.

APPENDIX C

Business Rules

Request and Response Data Elements

The relationship of all data elements contained in the online insurance verification messages follow. Further documentation can be obtained by contacting the Accredited Standards Committee (ASC) X12 at <http://www.x12.org/>.

Mandatory	M
Optional	O
Relational*	X

***Relational** – If a parent element is used, a value must be provided in the Relational field (relating the child element to the parent element). This is called a parent/child relationship.

Example: *Address is an Optional (O) data element, so it is not required. However, should the address be provided, the Relational (X) elements would be required. As shown below, for the parent element Address, the child elements would be Street Address, Subsite Address, City, Country Subdivision, State, Postal Code and Country.*

Please note, the child elements can become parent elements and have 'Relational' child elements as shown in the Subsite Address parent relationship with Apartment, Building, Department, Room, Floor and Suite.

```

<Address>
  <Street Address>
  <Subsite Address>
    <Apartment>
    <Building>
    <Department>
    <Room>
    <Floor>
    <Suite>
  <City>
  <Country Subdivision>
  <State>
  <Postal Code>
</Country>

```

Request Data Elements

Parent Element	Child/Sub-Parent Element	Child/Sub-Parent2 Element	Child/Sub-Parent3 Element	Child Element	Definition	Mandatory/Optional/Conditional M/O/X	Notes
Requestor Information						M	
	Organization				Name of the organization requesting the information	M	
		Name				M	
	Reason Details					M	
		Reason Code			The code identifying the reason why the request is needed	M	
		Tracking number			Unique identifier assigned by the Requestor	O	
	Policy Information					M	
		NAIC			The unique number assigned to each insurance company by the National Association of Insurance Commissioners	M	
		Policy Details				M	
			Verification Date		Date for which the Requestor is attempting to verify coverage	M	
			Unique Key		The unique number assigned to identify the insurance policy	M	
			Policy State		The state where the policy is assigned	M	
	Insured Information					O	
		Primary Name information				M	
			Parsed Name		The name of the party for whom information is being requested	M	
				Prefix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title before an individual's name	O	
				Given Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, first name	M	
				Middle Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, middle name	O	
				Surname	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, last name	M	
				Suffix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title after an individual's name	O	
			Drivers License		Describes unique identifier assigned to an individual and the licensing agency	O	
			FEIN		(Federal Employer Identification Number)The unique number assigned to a company/business by the US Federal Government	O	
		Additional Name information				O	
			Parsed Name		The name of the party for whom information is being requested	M	


				Prefix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title before an individual's name	O	
				Given Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, first name	M	
				Middle Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, middle name	O	
				Surname	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, last name	M	
				Suffix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title after an individual's name.	O	
			Drivers License		Describes unique identifier assigned to an individual and the licensing agency	O	
			FEIN		(Federal Employer Identification Number)The unique number assigned to a company/business by the US Federal Government	O	
	Address				Describes what is commonly known as the mailing address	O	
			Street Address		Specifies the set of details required to fully delineate a street number, as used in postal addressing schemes	X	
			Subsite Address		Detailed breakout of the information that is often found on the address lines of a mailing address such as apartment, building, department, floor, mail stop, room, or suite	X	
			Apartment		A single residence in a multi-unit dwelling	X	
			Building		A single structure	X	
			Department		A distinct, usually specified division of a large organization	X	
			Room		An area separated by walls or partitions from other similar parts of the building in which it is located	X	
			Floor		A story or level of building	X	
			Suite		A series of connected rooms used as a living unit	X	
			City		A word or phrase that describes a position or site	X	
			Country Subdivision		The highest level of subdivision within a country	X	
			Postal Code		Defines international Postal Code	X	
			Country		Code identifying country	X	
	Vehicle Information					O	
		Vehicle Details			Contains the information used to identify a specific vehicle	O	
			VIN		The Vehicle identification Number is a unique number the vehicle manufacturer assigns to a specific vehicle to provide identification for that specific vehicle	M	
			Make		Describes the manufacturer of the vehicle	O	
			Model		Describes the "kind" of vehicle a manufacturer makes	O	
			Year		Four position designation of the year. Describes when the vehicle was produced	O	





Response Data Elements

Parent Element	Child/Sub-Parent Element	Child/Sub-Parent2 Element	Child/Sub-Parent3 Element	Child Element	Definition	Mandatory/Optional/Conditional M/O/X	Notes
Requestor Information						M	
	Organization					M	
		Parsed Name				M	
		Name			Name of the organization requesting the information	M	
	Reason Details					M	
		Reason Code			The code identifying the reason why the request is needed	M	
		Tracking number			Unique identifier assigned by the Requestor	O	
	Policy Information					M	
		Coverage Status			Describes the status of the coverage for the policy listed in the inquiry	M	
			Response Details		Details the result of the inquiry	M	
				Response Code	Describes the result of the inquiry	M	
				Unconfirmed Reason Code	Describes the reason for an unconfirmed response	O	
		NAIC			The unique number assigned to each insurance company by the National Association of Insurance Commissioners	M	
		Policy Details				M	
			Verification Date		Date for which the Requestor is attempting to verify coverage	M	
			Unique Key		The unique number assigned to identify the insurance policy	M	
			Policy State		The state where the policy is assigned	M	
	Insured Information					O	
		Primary Name information				M	
			Parsed Name		The name of the party for whom information is being requested	M	
				Prefix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title before an individual's name	O	
				Given Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, first name	M	
				Middle Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, middle name	O	
				Surname	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, last name	M	
				Suffix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title after an individual's name	O	
			Drivers License		Describes unique identifier assigned to an individual and the licensing agency	O	

			FEIN		(Federal Employer Identification Number) The unique number assigned to a company/business by the US Federal Government	O	
		Additional Name information				O	
			Parsed Name		The name of the party for whom information is being requested	M	
				Prefix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title before an individual's name.	X	
				Given Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, first name	M	
				Middle Name	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, middle name	O	
				Surname	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept, last name	M	
				Suffix	A word or phrase that constitutes the distinctive designation of a person, place, thing, or concept; title after an individual's name	O	
			Drivers License		Describes unique identifier assigned to an individual and the licensing agency	O	
			FEIN		(Federal Employer Identification Number)The unique number assigned to a company/business by the US Federal Government	O	
		Address			Describes what is commonly known as the mailing address	O	
			Street Address		Specifies the set of details required to fully delineate a street number, as used in postal addressing schemes	X	
			Subsite Address		Detailed breakout of the information that is often found on the address lines of a mailing address such as apartment, building, department, floor, mail stop, room, or suite	X	
				Apartment	A single residence in a multi-unit dwelling	X	
				Building	A single structure	X	
				Department	A distinct, usually specified division of a large organization	X	
				Room	An area separated by walls or partitions from other similar parts of the building in which it is located	X	
				Floor	A story or level of building	X	
				Suite	A series of connected rooms used as a living unit	X	
			City		A word or phrase that describes a position or site	X	
			Country Subdivision		The highest level of subdivision within a country	X	
			Postal Code		Defines international Postal Code	X	
			Country		Code identifying country	X	
	Vehicle Information					O	
		Vehicle Details			Contains the information used to identify a specific vehicle	O	
			VIN		The Vehicle identification Number is a unique number the vehicle manufacturer assigns to a specific vehicle to provide identification for that specific vehicle	M	
			Make		Describes the manufacturer of the vehicle	O	
			Model		Describes the "kind" of vehicle a manufacturer makes	O	
			Year		Four position designation of the year. Describes when the vehicle was produced	O	

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 schema 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)**.
-  **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

The Model User Guide for Implementing Online Insurance Verification Version 5.0 published on 4/18/2012 has been revised as follows:

- Deleted the **Data Dictionary** on page 16. Replaced it by adding **Appendix C - Business Rules** pages 26-30.
- Pages 2-4: The **Unknown Carrier** request and the general program overview were updated for clarity.
- Page 7:
 - The term **state reporting model** was replaced by **insurance verification model**.
 - The term **insurers** was replaced by **insurance companies**.
 - The term **state reporting model** was replaced by **a model requiring insurance policy data reporting**.
 - The term **requesting parties** was replaced by **authorized entities, such as Departments of Motor Vehicles**.
 - The term **elements** was replaced by **process**.
- Page 8: The swim lane 'last updated' date and 'version' changed. 'Requestor' was added to left column.
- Page 9:
 - The term **insureds** was replaced by **customers provided insurance through a commercial policy**.
 - The term **Standards** organizations was replaced by **national standards development** organizations.
 - ACCORD's website was added.
- Page 11: **Function** was corrected to **functional**.
- Page 14: **Commercial insureds** was corrected to **commercially insured customers**.
- Page 16: **Sent back** was replaced by **transmitted**.

Bibliography

- 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.