Model User Guide for Implementing Online Insurance Verification

Using Web services to verify auto insurance coverage

Version 2.0
April 15, 2007

Insurance Industry Committee on
Motor Vehicle Administration

Executive Summary

IICMVA's ***Model User Guide for Implementing Online Insurance Verification*** serves as a technical follow up to the Committee's 2004 white paper publication entitled, ***Online Insurance Verification – Using Web Services to Verify Auto Insurance Coverage Version 1.0*** ***(*** http://www.iicmva.com/websvc.pdf ***)***.

In the 2004 white paper, IICMVA identified the following benefits of online insurance verification:

- Jurisdictions could 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 or as soon as possible following the binding of a bound application.
- Jurisdictions could incorporate online verification systems into their license plate renewal programs.
- There would be 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 would be protected within the confines of each insurance carrier's IT environment.
- The matching limitations and data integrity issues of current state reporting programs would be reduced.
- Customer service would be improved because primary search criteria would be based on the business rules within each company.
- Commercial insurance carriers would be in a better position to comply with state mandates.
- Carriers would realize the cost effective use of resources since an inquiry system would be built one time for all states, leaving room for simple upgrades as future needs arise.
- Privacy will be protected: Only designated, legally authorized entities will have access. The information provided will be very limited and state of the art technological safeguards, such as the latest methods of encryption, will be included.

IICMVA believes that Web service technology should be explored as a solution to address the need by state agencies to verify minimum financial responsibility coverage.

This model guide serves as a technical "how to" for implementing an auto insurance verification program using externally consumable Web services. The guide has been developed only by insurance company representatives from the IICMVA, and it has been written as a vendor-neutral resource. Since it is based on open standards, the guide provides state jurisdictions with the choice of either developing an online verification program with internal or third party resources.

Table of Contents

1.0 Introduction to the Model User Guide

1.1 Revisions to Version 1.0 Document

The *Model User Guide for Implementing Online Insurance Verification Version 1.0* published on 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:

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

  2. 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.

  3. 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.

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

  5. A comment is provided in the *System Distributes Communication* section to state that financial responsibility limits are not returned to the authorized requester.

- 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.

1.2 User Guide Purpose

The purpose of this guide is to provide insurance companies, state motor vehicle administrations (MVAs), or their respective agents with the information needed to conduct online auto financial responsibility coverage verification via Web service applications.

This guide provides both business and technical information to define how ***authorized requesters*** (e.g., motor vehicle departments) can submit insurance verification requests to Web services hosted by insurance carriers participating in this program. The first section will focus on the general business requirements. Subsequent sections will address the technical recommendations and requirements to be followed by party intending to implement this solution.

> ***Note:*** Departments of Motor Vehicles (DMV) are the only authorized requesting parties recognized by insurers providing this online insurance verification service. The reason is DMVs are the keepers of records for motor vehicle administration (MVA) purposes. DMVs are the conduit through which other state agencies access MVA information; therefore, DMVs will decide how to shape their user IDs.

1.3 Program Goal

The goals for online insurance verification via Web services include:

- Providing an accurate, flexible, and simple method of auto liability insurance verification 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.

1.4 Program Purpose

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

The current state reporting model requires insurance carriers to report insurance information so that it can be 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 coverage.

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

IICMVA's vision includes simple online applications that can support single policy inquiries submitted through Web service applications by an interconnection of authorized trading partner systems (i.e., insurance carriers and DMVs).

Under the online insurance inquiry model, the presence of minimum financial responsibility coverage may be verified when an authorized requester is presented with a financial responsibility event for a driver.

Online verification bypasses the need to identify a match between 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 authorized requesters to go directly to the source of insurance information -- the insurance companies themselves.

1.5 Program Overview

For the online insurance verification model, IICMVA identifies the standards, processes, requirements, and technical specifications necessary to interact with externally consumable Web services hosted by insurance carriers. In addition, IICMVA defines the confirmation responses that state agencies may receive in response to their insurance inquiry requests.

IICMVA does not define the ***user interface*** or method through which an authorized requester submits a coverage confirmation request to these Web services.

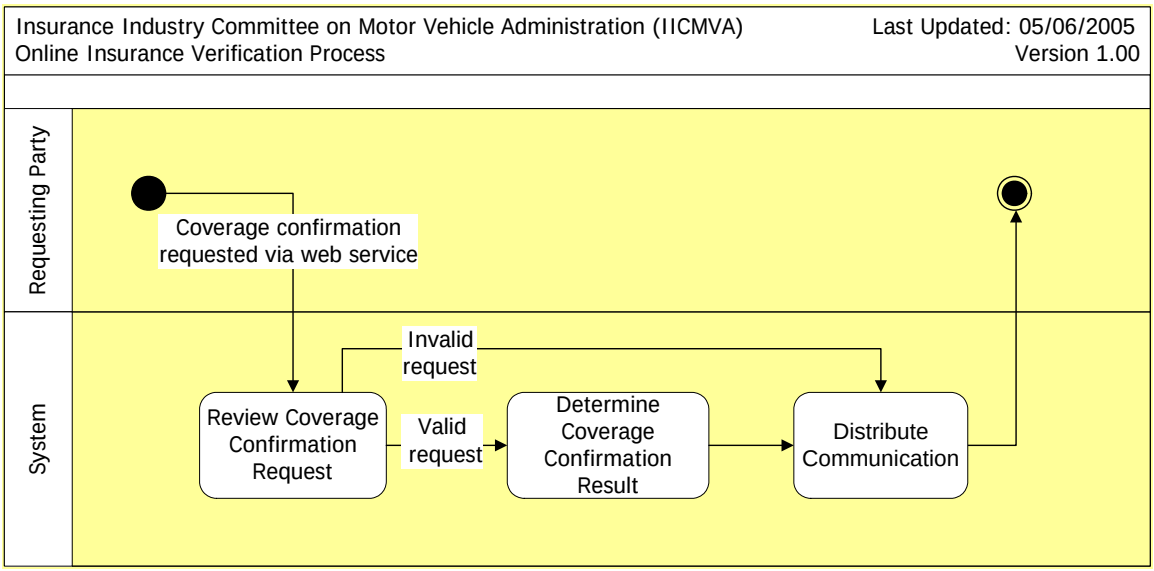
When presented with a financial responsibility event, an authorized requester simply submits a standardized, ***coverage confirmation request*** to the Web service of a participating insurance carrier. In turn, the insurance carrier replies with a standardized, ***coverage confirmation response***.

> ***Note:*** The insurance company's response indicates whether it can confirm minimum financial responsibility coverage 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.*

2.0 Inquiry Process

This section describes the inquiry process that occurs when an authorized party submits a coverage confirmation request to an insurance carrier's Web service application.

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



2.1 Authorized Requesting Party Submits Coverage Confirmation Request

An authorized requesting party submits a coverage confirmation request or inquiry 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 T.2.2.2).

The message content key from the requesting entity may include ***optional*** data elements (Functional and Technical Requirements T.2.2.3).

2.2 System Validates Coverage Confirmation Request

The Web service application of the participating insurance carrier validates the coverage confirmation request to confirm the presence of minimum financial responsibility coverage:

- The system verifies that the coverage confirmation request is from an authorized requesting party.

- The system verifies that the coverage confirmation request has the required message content or policy information.

- The system verifies that the policy information provided by the coverage confirmation request is in the correct format.

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

UNCONFIRMED results for invalid coverage requests may be supplemented with ***reason messages*** available from the ANSI X12/XML or ACORD standard specifications. Please refer to those standards bodies for liability available ***reason messages***.

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

2.3 System Determines Coverage Confirmation Result

The Web service application takes the valid request and evaluates whether policy coverage was present:

- The system evaluates whether the policy information provided in the coverage confirmation request is present on the insurance carrier's database.

- The system determines if minimum financial responsibility coverage was present and the policy was active on the requested coverage confirmation date.

2.4 System Distributes Communication

For valid coverage confirmation requests,

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

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

The term **UNCONFIRMED** does not necessarily mean there is no minimum financial responsibility coverage 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 coverage requests may be supplemented with ***reason messages*** available from the ANSI X12/XML or ACORD standard specifications. Please refer to those standards bodies for available ***reason messages***.

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 coverage confirmation result since it would have to travel over the public Internet. However, the coverage confirmation result does provide what is most important: confirmation of auto financial responsibility insurance coverage based on the minimum financial responsibility limits required by each state. Financial responsibility limits will not be passed back to the authorized requester because internal rules should take the state code of the authorized requester into consideration when confirming 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 authorized requesters to confirm coverage in an online environment directly with the source of the policy information—the insurance carrier.

IICMVA believes this is a more accurate approach.

3.0 Requirements

3.1 Business Requirements

The foundation for the inquiry process described in Section 2.0 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 this Appendix A. These requirements are complimented by the function and technical requirements also located in Appendix A.

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 insurance coverage 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 coverage, 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 coverage will be sent back to the requesting entity for appropriate action.

Glossary

Open Standards

- ***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 confirmation 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).***

- ***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."***

- ***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.

- ***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.

- ***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***.

- 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.

- ***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.

Internet

- ***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***.

- ***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.

Security

- ***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 authorized requester.

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

- ***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.

Appendix A - Technical Processes and Considerations

A. 1 Technical Overview

In Section 1.4, "Program Purpose", it was identified that this proposal offers an alternative solution to insurance verification by the individual states through the use of web services. 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 prior to the Appendices.

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***)

A.2 Functional and Technical Requirements

The following requirements are complimentary to the Business Requirements in Section 3.0 and provide the foundation for the Technical Specifications in the next section.

Functional and Technical Requirements	
ID #	Description
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 coverage.
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 7 X 24 hour availability.
T2.5.1	The system will provide the quickest response time possible during the busiest hour of the day while the system is under load.
F3.1	Carriers will individually decide at what level they will confirm coverage to a requesting entity: *policy level* or *vehicle level*.
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 entity will include the following mandatory data elements: • Policy Key ***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.* • Vehicle Identification Number (VIN) ***Note:*** *VIN is used by carriers that will be confirming coverage at the vehicle level. Some carriers may choose to confirm coverage at the policy level.* • NAIC (National Association of Insurance Commissioners) Code • Requested Confirmation Date

T3.2.4	The message content key from the requesting entity may include the following optional data elements: ▪ Tracking / Reference Number ***Note:*** *The system shall provide the ability to accept and return a reference number so that an authorized requester can tie together a coverage confirmation request with a coverage confirmation response.* • Drivers License Number • Named Insured Name • Address: 1. Street/PO Box 2. City 3. State 4. Zip • Vehicle Make • Vehicle Model • Vehicle Year • Federal Employer Identification Number (FEIN)
F4.1	A legal trading partner agreement between insurance carriers and the requesting entity will be required to exchange data via the Web Service.
F4.2	The requesting entity 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.
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
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 confirm coverage, 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/.

A.3 Technical Specifications

This section describes the technical processes that must be considered if an authorized requesting party wishes to submit a coverage confirmation 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 technical specifications identified in Section 3.0 of 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 coverage on their own customers.
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[1]
4	It will be the responsibility of the requesting entity 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.
6	**Maintain multiple environments**
6.1	All jurisdictions and carriers must maintain a minimum of two identical environments (one test and one production).

A.4 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.

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

Standard interfaces are crucial because they allow authorized requesters 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 authorized requester 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 requester 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 authorized requester 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 authorized requesters 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 requester.

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 requesters 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 requester's certificate, and the requester must trust the insurance company's certificate. Each customer or client 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:Pa
                                ssword>
                        <wsse:Nonce>x/8L/bSduwsMdYmi+cP9iw==</wsse:Non
                ce>
                        <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.

A. 5 Authorized Requesting Party Responsibilities

Each authorized requesting party or state is responsible for developing an insurance verification ***Web service client*** based on the standards identified in Section 4.1 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 requester'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 authorized requester'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 authorized requester'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 authorized 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 authorized requester 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.

Consider Creating and Maintaining a list of Technical Contacts

Since Web Services should be highly available, the IICMVA recommends maintaining a list of technical contacts that:

- Are available outside of normal business hours.
- Are familiar with Web Services and should be able to assist with problems.

A.6 Implementation Scenarios for Authorized Requesting Parties

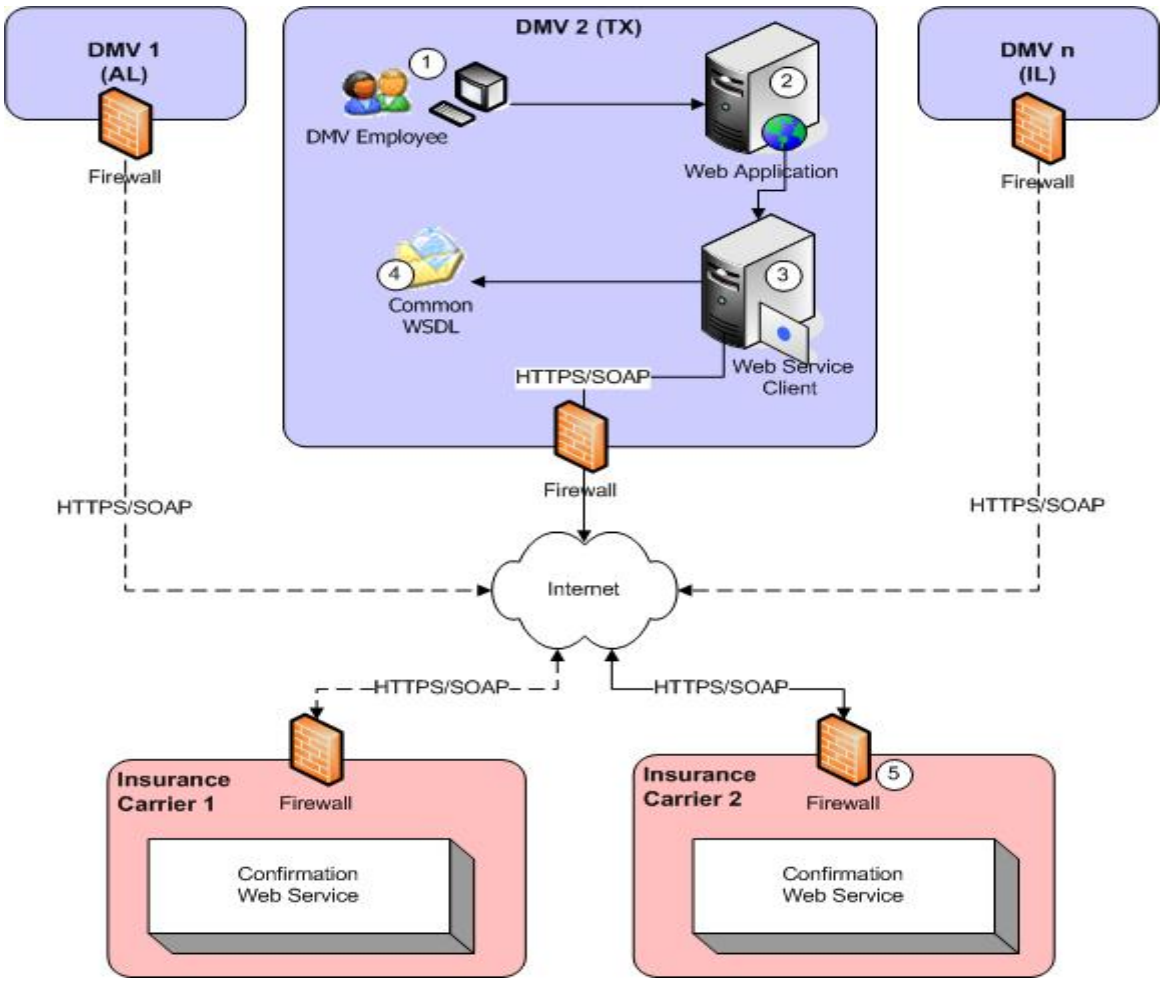
The following diagrams have been provided to illustrate the different possibilities that exist when an authorized requester implements a Web service client using internal resources or a third party vendor.

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 authorized requesting party requests the current status of insurance coverage from an insurance carrier. The request is fully automated and enabled by Web services. The coverage request is exchanged directly between a State DMV (authorized requester) 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.

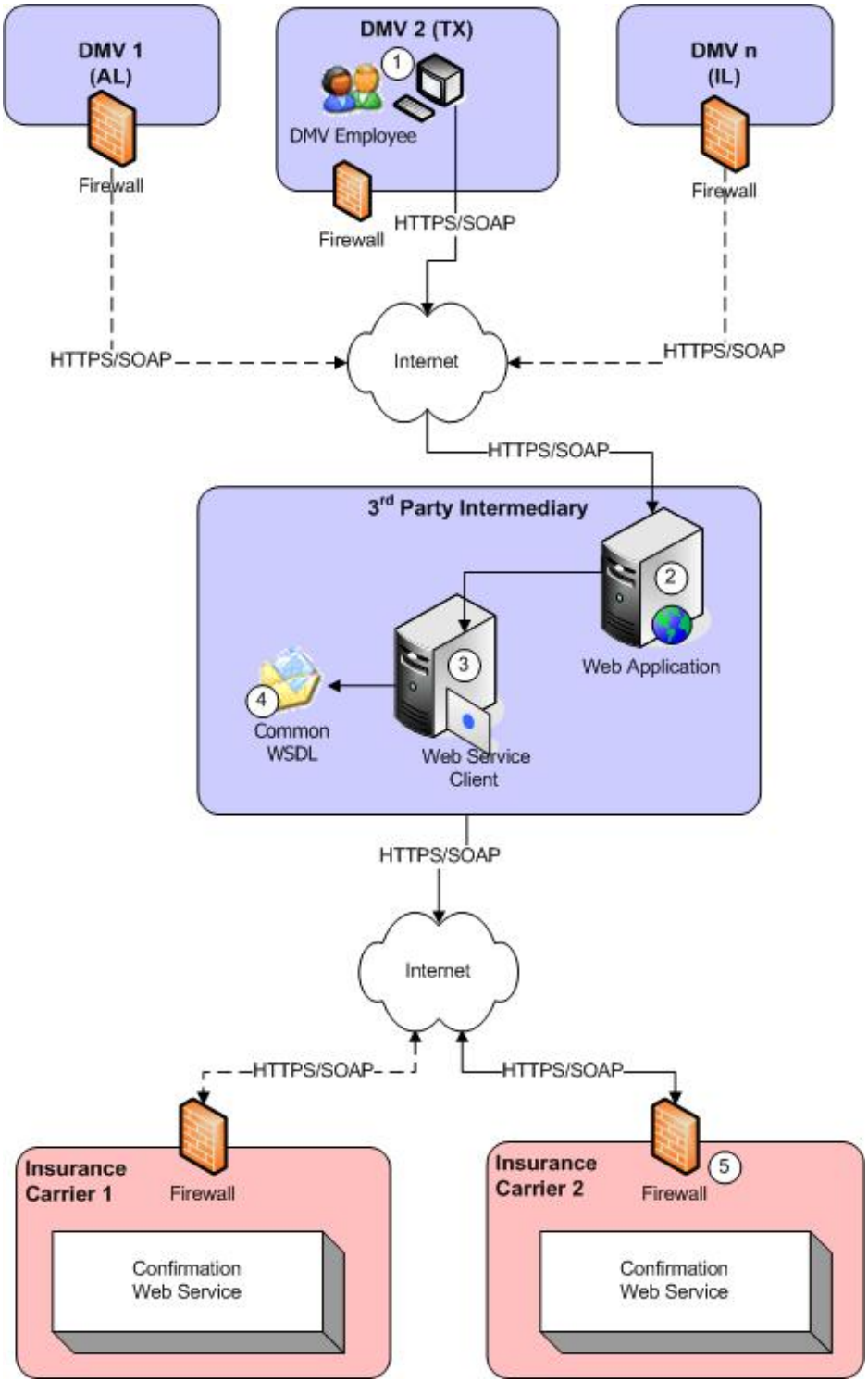
3. There is a logical separation between the Web application and the Web service. Although not required, the Web application and Web service can be located on separate physical servers if desired.

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 current status of insurance coverage 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 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. 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 confirmation to the DMV.

A.7 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.

A.8 Service Level Agreement (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 authorized 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.

Due to the recent advent of externally consumable Web services, an historical SLA has not been established for the insurance verification application.

IICMVA recommends a testing period be established so that insurance carriers and requesting parties can come to a mutually beneficial agreement based on consumption patterns.

A.9 Impact of Batch Requests

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

If a requester 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 requester 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 authorized requesting party as well. Instead of simply creating a Web service client to submit requests to insurance carrier Web services, authorized requesters 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.

A.10 Testing Procedures

To ensure standardization across carriers and jurisdictions, a standard test strategy and test plan should be utilized. For the initial implementation, the test strategy and plans are found in Appendices A and B respectively. These documents may be modified and updated to meet the needs of the system as it enhanced.

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.