U.S. Department
of Transportation

**Federal Aviation
Administration**

U.S. Department of Transportation
Federal Aviation Administration

Standard Practice

PREPARATION OF
WEB SERVICE REQUIREMENTS DOCUMENTS

FOREWORD

This standard is approved for use by all Departments of the Federal Aviation Administration (FAA).

This standard specifies the minimum acceptable content for preparing FAA Web service requirements documents (WSRD).

This standard is one of several related standards that together define FAA's requirements for describing and registering services. A Handbook entitled *Using FAA Standards to Describe and Register Web Services* (FAA-HDBK-008) [5] provides additional guidance for using these standards.

This standard has been prepared in accordance with FAA-STD-068, Department of Transportation Federal Aviation Administration, *Preparation of Standards* (December 2009) [12].

Comments, suggestions, or questions on this document shall be addressed to:

> Federal Aviation Administration
> Office of Engineering Services, ANG-B
> 800 Independence Avenue, SW
> Washington, DC 20591

Table of Contents

List of Figures

List of Tables

iii

1 SCOPE

This standard defines the content and structure of a Web Services Requirements Document (WSRD). The WSRD provides the details needed to specify requirements for a <u>Web service</u> that is part of the FAA's implementation of a <u>service-oriented architecture</u> (SOA).

- This standard does not prescribe or suggest any technological solutions for developing a Web service.

- This standard does not specify any configuration management procedures or policies to which the developed WSRD may be subjected.

1.1 Introduction

Over the last decade, the <u>net-centric</u> paradigm has become the predominant motivating factor in the development of information technologies (IT) for the entire FAA <u>organization</u>. The most prominent type of architecture that allows FAA to realize the major objectives of a net-centric approach is a <u>service-oriented architecture</u>, or SOA. SOA has emerged as the premier integration and architecture framework in today's complex computing environment. It enables organizations to leverage investments by developing new services from existing infrastructures or systems.

The introduction of SOA has presented a number of challenges in different areas of IT, including the area of identifying and describing requirements for the development and/or acquisition of <u>Web services</u>. And although the FAA has a long and well-established set of practices for capturing requirements for distributed information systems, these practices are not always sufficiently tailored to the nuances of Web service solutions.

For example, the Interface Requirements Document (IRD) content and structure prescribed by FAA-STD-025 <u>[6]</u> have been well-suited for identifying requirements for interaction between two systems or processes connected via a dedicated communication link or across a switched network using mutually agreed-upon conventions. Web services are different in that they usually offer capabilities to a broad range of <u>service consumers</u>, some of whom may not even be identified at the requirements development stage and who may use various platforms for developing and implementing software components. These and other features specifically typical of a SOA environment call for new formats and artifacts for describing requirements for Web services.

The purpose of this standard is to fill this gap by establishing a uniform content and structure for specifying a set of requirements, rendered as a Web Service Requirements Document (WSRD) usually created by the FAA, which identifies the necessary provisions for developing a Web service, usually performed by government contractors or vendors.

1.2 Intended Audience

The intended audience for this standard includes architects, decision makers, analysts, requirements developers, and implementers responsible for developing FAA <u>Web services</u>.

1.3 Basic Concepts

This section introduces major terms, concepts, and ideas relevant to this standard. Many service-related terms such as SOA, Web service, service interface, and so forth have become overloaded with different meanings throughout industry and government <u>organizations</u>, including the FAA, resulting in confusion. To set the boundaries of requirements for a <u>WSRD</u> and to ensure that the WSRD will be effective, it is first necessary to establish a clear and rational understanding of these terms.
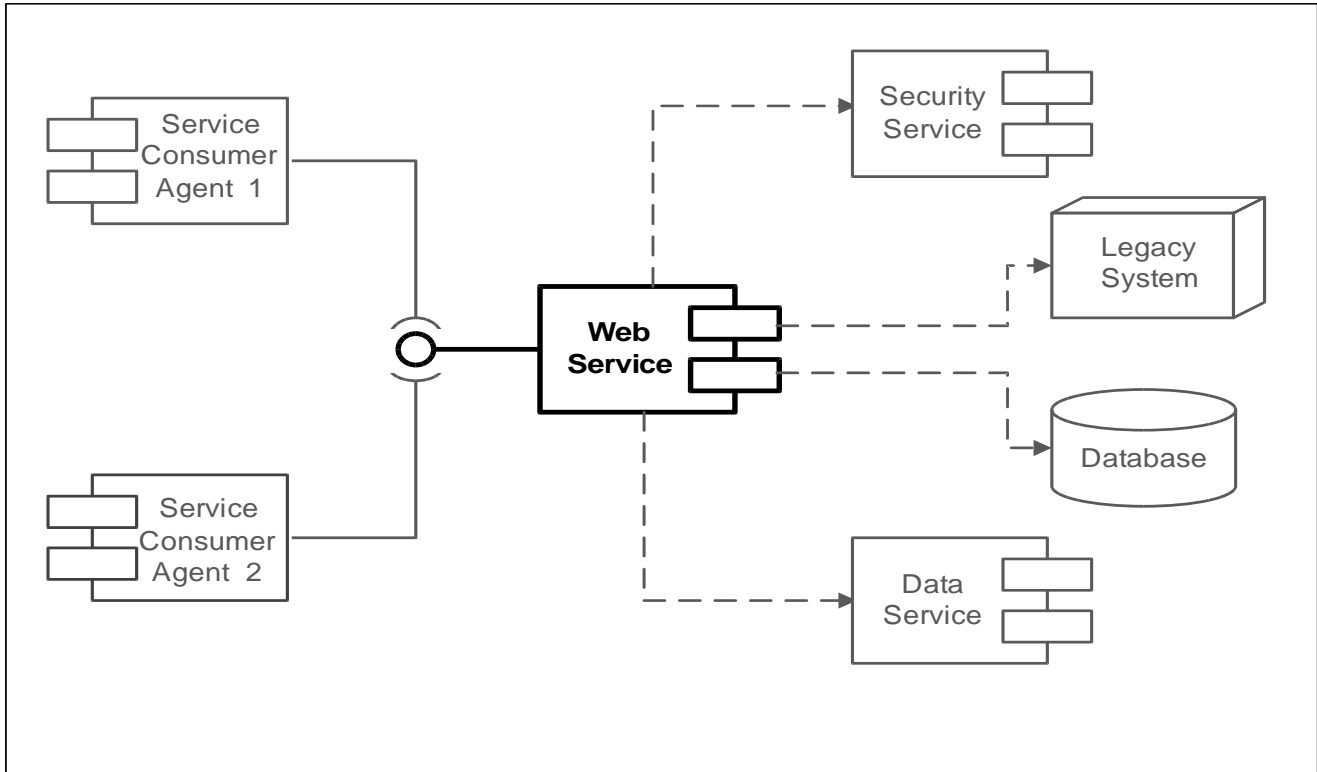
1.3.1 Service-Oriented Architecture (SOA)

For the purpose of this standard, SOA is understood to be an architecture style that is based on loosely-coupled interoperable reusable software components commonly referred to as "services". From FAA's perspective, the major motivation for SOA is to transform tightly-coupled systems in which all "system elements (e.g., programs, databases, subsystems, etc.) are highly dependent on each other and are generally interconnected through individual, point-to-point interfaces" [15] into a set of loosely-coupled services that can be created from an existing IT infrastructure of systems and can be used and reused across the FAA to leverage existing investments and promote interoperability among heterogeneous technologies and organizational domains.
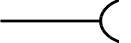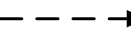
The following is a list of major SOA characteristics and their consequent relevance to the scope of a WSRD. Note: SOA characteristics that are not pertinent to the context of a WSRD are not elaborated here.

- Loosely-coupled – Dependencies between interrelating SOA components are minimized. This means that "services are designed with no affinity to any particular service consumer" [34], that is, a SOA service has no intrinsic intelligence about consumers of that service. As a result, requirements levied on other SOA components are outside the scope of a WSRD, although it may describe the information pertaining to interaction with these components.

- Interoperable – SOA components should be able to interact across heterogeneous computational platforms, operating systems, and programming languages. This is achieved through adherence to a common set of standard protocols (mainly non-proprietary, i.e., "open"). As a part of its requirements, a WSRD identifies data, messaging, communication, security, and other protocols.

- Autonomous – SOA components encapsulate the implementation of their own business functions and, recognizing that the other interacting "components neither know nor care how services perform their function, they merely anticipate that they return the expected result" [35]. As a logical consequence of this principle, a WSRD does not impose any requirements pertaining to the implementation of other components.

- Reusable – SOA components are realized as autonomous and self-contained IT assets and as such can be reused by an undefined number of service consumers even in contexts often unknown at design time. Modeling SOA components so they can be reused across various domains is ordinarily a subject of architectural documentation which precedes development of a WSRD.

- Discoverable – SOA components should be discoverable, which means that there exist processes through which a service consumer may search for and find (i.e., discover) the service. Discoverability is a key attribute of a SOA environment and is usually provided by the organization that is responsible for the support and governance of the SOA infrastructure; therefore it is outside the scope of a WSRD.

Figure 1 depicts a typical SOA integrated environment with a Web service component (the subject of a WSRD) and illustrates some of the points described above. The Web service in the figure may be used to expose some legacy system and/or retrieve or store data in some database. It may invoke other services that the SOA environment may have established, in this case a data service and a security service. There are also two service consumers that utilize the Web service through the use of a service interface.

FIGURE 1. Web service within SOA integrated environment

⎯⎯○	This symbol represents an interface that a component, in this case a Web service, extends to another component, in this case a service consumer. The WSRD specifies requirements for this interface.
⎯⎯(	This symbol (a.k.a. socket) represents an interface that a component, in this case a requester agent, needs to implement in order to use the service.
– – – →	This symbol (a unidirectional association) indicates that two components are related, but only one, in this case the Web service, knows that the relationship exists. These relationships (dependencies) may be specified in the WSRD.
○⎯ **Web Service**	Bold outlines represent the extent of coverage by the WSRD. Other components are optional; they represent possible SOA-based implementations, and they are described in their own respective documentation (e.g., software requirement documents, database administration documents, etc.) which is outside the scope of the WSRD.

3

1.3.2 Web Service

Services are primary architectural assets and central artifacts of an SOA. Although services in SOA could be implemented using various enabling technology approaches (e.g., OMG CORBA, MS DCOM, MS .NET, Java EE, Sun Jini, etc.); a solution that leverages usage of Web and Internet-based standards (e.g., XML, HTTP, JMS, SOAP, etc.) has become a predominant approach in implementing SOA-based solutions. Services using this approach are commonly referred to as Web services. (Note: in SOA documentation, the term "Web service" is often used synonymously with the term "service".) Because this standard is about Web services, the term "service" is also used herein to mean "Web service" unless explicitly indicated otherwise.

The World Wide Web Consortium (W3C) defines a Web service as a software component "whose interfaces and bindings are capable of being defined, described and discovered by XML artifacts and supports direct interactions with other software applications using XML-based messages via Internet-based protocols" [39].

It is also worth noting that because a Web service is a special case of SOA service as presented in section 1.3.1, Web services are also inherently loosely-coupled, interoperable, autonomous, reusable, and discoverable.

Another very important aspect of Web services is that they are self-describing. "Self-describing" means that a service provides a service consumer with all of the relevant information that is necessary for using the service.

Recapping all of the above and taking into consideration the heterogeneous and rapidly evolving nature of services as well as current trends in implementing SOA in the FAA, for the purpose of this standard we assert the following:

> A *Web service* is a platform-independent, loosely-coupled software component designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format. Other systems interact with the Web service in a manner prescribed by its description by means of XML-based messages conveyed using Internet transport protocols in conjunction with other Web-related standards. (Adapted from [40])

1.3.3 Web Service Interface

The service interface – another term having multiple interpretations in industry and in the FAA – is a fundamental, definitive component of a Web service. In a very broad sense, the term interface means "a point of communication between two or more processes, persons, or other physical entities" [13]. More specifically, in information technology an "interface might be a hardware connector used to link to other devices, or it might be a convention used to allow communication between two software systems" [18], or a "shared boundary between two functional units, defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges, and other characteristics, as appropriate" [23].

In the FAA the concept of interface has ordinarily been subdivided into various types of interfaces based on their focus on technology or characteristics of interrelated components. (See for example the definitions of Physical Interface, Facility Interface, Analog Interface and others that occur in [6].) In keeping with the FAA's approach, we also offer a definition for Web service interface to be used throughout this standard.

As mentioned in the previous section, one of the main principles of SOA is loose-coupling among SOA components. A logical consequence of loose-coupling is that "any entity that a Web service may interact with may not exist at the point of time the Web service is developed" [27]. That

means that a Web service interface is not a binding agreement or a shared convention between two or more components, but rather it is a description of the mechanics of the message exchange (e.g., message formats, fault processing, etc.).

Another key feature of SOA is that a service interface is an "abstraction"; that is, the service interface hides the service implementation from a service consumer ("black box" approach). A service interface only describes a collection of messages which "does not contain information how to accomplish, for example, some data manipulation but only contains the data to be manipulated without caring how the data is to be manipulated" [35].

Summarizing all of the above, we assert the following:

> "A *Web service interface* is an abstract boundary that a Web service exposes. It defines the types of messages and the message exchange patterns that are involved in interacting with the Web service, together with any conditions implied by those messages" [36].

1.3.3.1 Service Interface Description

This standard follows the abstract model of interface description defined by the W3C in the Web Service Description Language (WSDL) specification [38]. The WSDL specification provides a framework for describing a Web service and, more specifically, a service interface in terms of the W3C Abstract Component Model. This model "defines the abstract interface of a Web service as a set of abstract operations, each operation representing a simple interaction between the consumer and the service. Each operation specifies the types of messages that the service can send or receive as part of that operation. Each operation also specifies a message exchange pattern that indicates the sequence in which the associated messages are to be transmitted between the parties" [37].

For the purpose of this standard, the interface definition model is asserted as follows (see also Figure 2):

"An *interface* groups together operations without any commitment to transport or wire format" [38], i.e., an interface is a "logical grouping of operations" [39]. Requirements for the interface should be presented in section 5.2 of a WSRD.

An *operation* is "a sequence of messages related to a single Web service action" [39] or, more specifically, "an interaction with the service consisting of a set of (ordinary and fault) messages exchanged between the service and the other parties involved in the interaction" [22]. Requirements for the operations should be presented in section 5.2.1 of a WSRD.

A *message* is an identifiable collection of units of information (data elements), presented in a manner suitable for communication, interpretation, or processing within a context of interacting SOA components. The content of messages (and faults) is rendered through a sequence of data elements. Requirements for the messages should be presented in section 5.2.2 of a WSRD.

A *data element* is "a unit of data for which the specified definition, identification, representation and permissible values are specified by means of a set of attributes" [19]. Note: in the WSDL model, the term "type" is used to denote this concept; this standard uses the term "data element" in order to stay consistent with FAA practices. Requirements for the data elements should be presented in section 5.2.4 of a WSRD.

A *fault* is a message that is returned as a result of an error that prevents the service from implementing a required function. A fault usually contains information about the cause of the error. Requirements for the faults should be presented in section 5.2.3 of a WSRD.
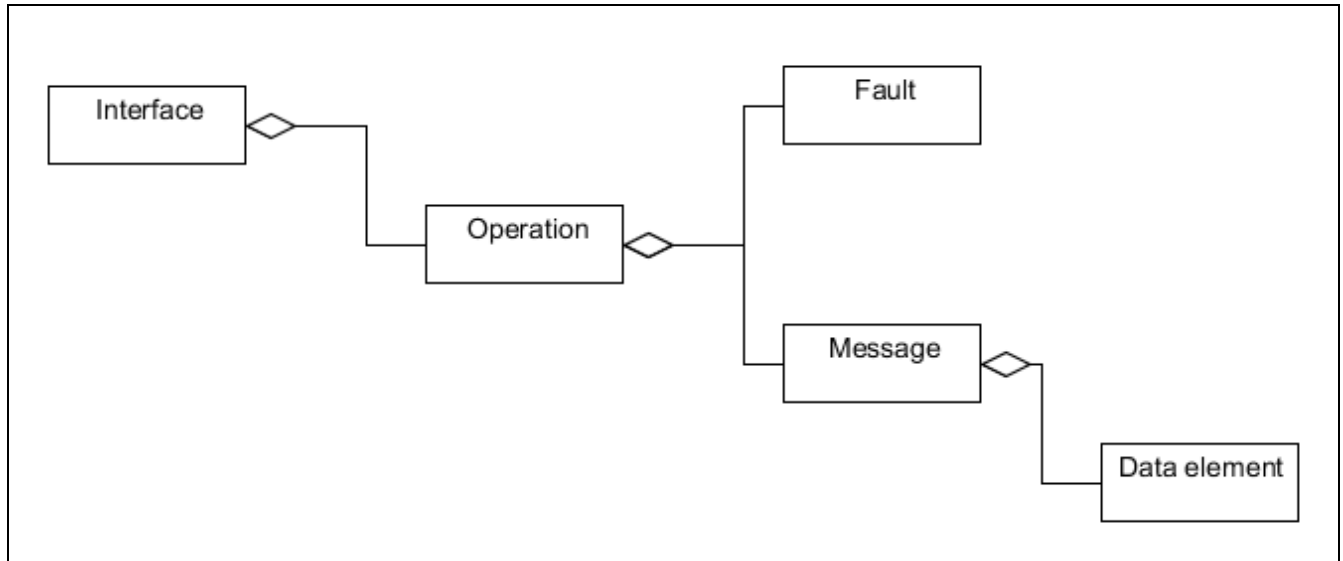
FIGURE 2. Web service interface conceptual diagram

2 APPLICABLE DOCUMENTS

2.1 Government Documents

[1]   FAA Order 1000.36, FAA Writing Standards, 31 March 2003.
       http://www.faa.gov/documentlibrary/media/order/branding_writing/order1000_36.pdf

[2]   FAA Order 1370.92A, Password and PIN Management Policy, 6 August 2010.
       http://www.faa.gov/documentLibrary/media/Order/1370.92A.pdf

[3]   FAA Order 1375.1E, Information/Data Management, 16 November 2011.
       http://www.faa.gov/documentLibrary/media/Order/1375.1%20E.pdf

[4]   FAA Order 1700.6C, FAA Branding Policy, Use of the FAA Logo, FAA Signature, and DOT Seal,
       11 September 2006.
       http://www.faa.gov/documentLibrary/media/order/branding_writing/Branding_Order_17006.
       pdf

[5]   FAA-HDBK-008, Using FAA Standards to Describe and Register Web Services, 4 February
       2011.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[6]   FAA-STD-025f, Preparation of Interface Documentation, 30 November 2007.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[7]   FAA-STD-060b, Data Standard for the National Airspace System, 8 March 2004.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[8]   FAA-STD-063, XML Namespaces, 1 May 2009.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[9]   FAA-STD-064, Web Service Registration, 1 May 2009.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[10]   FAA-STD-065, Preparation of Web Service Description Documents, 26 February 2010.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[11]   FAA-STD-066, Web Service Taxonomies, 26 February 2010.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[12]   FAA-STD-068, Preparation of Standards, 4 December 2009.
       http://207.67.203.68/F10011Staff/OPAC/index.asp

[13]   Federal Standard 1037C, Glossary of Telecommunication Terms, 7 August 1996.
       http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm

[14]   NAS System Engineering Manual, Version 3.1, 6 June 2006.
       http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/operations/syse
       ngsaf/seman/

[15]   U.S. Department of Health and Human Services Centers for Medicare and Medicaid (CMS) Medicaid IT Architecture Part III - Technical Architecture, Chapter 3 - SOA Concept, March 2006.
http://www.hits.virginia.gov/hits-devel/hie_plan_2010/TIC/Part%20III%20Chapter%203%20-%20SOA%20Concept.pdf

[16]   U.S. Government Printing Office Style Manual, 30th edition 2008.
http://www.gpoaccess.gov/stylemanual/

2.2 Non-Government Documents

[17]   DCMI Glossary, Dublin Core Metadata Initiative, User Guide Committee, 23 April 2004.
http://dublincore.org/documents/usageguide/glossary.shtml

[18]   Free On-line Dictionary of Computing, Denis Howe, 2010.
http://foldoc.org

[19]   ISO/IEC 11179-1, Information Technology – Metadata Registries (MDR) – Part 1: Framework, 15 September 2004.
http://metadata-standards.org/11179/

[20]   ISO/IEC 12207, Information Technology – Software Life Cycle Processes, 1995.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=21208

[21]   ISO/IEC 6523-1, Structure for the Identification of Organizations and Organization Parts, 1998.
http://www.iso.org/iso/catalogue_detail?csnumber=25773

[22]   ISO/IEC 7498-1, Open Systems Interconnection - Basic Reference Model, 1994.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=20269

[23]   ISO/IEC CD 20944-002, Information Technology – Metadata Interoperability and Bindings (MDIB) – Part 002, Common Vocabulary, 12 April 2004.
http://jtc1sc32.org/doc/N1101-1150/32N1105T-CD20944-002.pdf

[24]   Glossary of Security Terms, SANS Institute, August 2011
http://www.sans.org/resources/glossary.php

[25]   OASIS Reference Model for SOA 1.0, 12 October 2006.
http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf

[26]   OASIS Reference Ontology for Semantic Service Oriented Architectures, Public Review 1, 5 November 2008.
http://www.oasis-open.org/apps/group_public/download.php/29909/Reference Ontology for Semantic Service Oriented Architectures_Public_Review_1.doc

[27]   Position Papers for the W3C Workshop on Web Services: W3C Web Services Team: April 3, 2001.
http://www.hpl.hp.com/techreports/2001/HPL-2001-73.pdf

[28]   RFC 2119, Key words for Use in RFCs to Indicate Requirement Levels, Network Working Group, March 1997.
http://www.rfc-editor.org/rfc/rfc2119.txt

[29]   RFC 2828, Internet Security Glossary: Network Working Group, May 2000.
http://www.ietf.org/rfc/rfc2828.txt

[30]   (Reserved)

[31]   RFC 3935, Mission Statement for the Internet Engineering Task Force (IETF), Network Working Group, October 2004.
http://www.ietf.org/rfc/rfc3935.txt

[32]   RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, Network Working Group, January 2005
http://www.rfc-editor.org/rfc/rfc3986.txt

[33]   Service Oriented Architectures for All (SOA4All) Glossary, 2008.
http://www.soa4all.eu/glossary.html

[34]   SOA Definition and Principles, R. W. Schulte and Y. V. Natis, Gartner Group, 2003.
No longer available online.

[35]   State of the Art in Developing Applications Using Services, Mikko Raatikainen, Helsinki University of Technology
http://www.soberit.hut.fi/mjraatik/Presentations/T-76273_Spring2005/T-76273_report.pdf

[36]   Web Services Architecture, W3C Working Group Note, 11 February 2004.
http://www.w3.org/TR/ws-arch

[37]   Web Services Description Language (WSDL) Version 2.0 Part 0: Primer, W3C Recommendation, 26 June 2007.
http://www.w3.org/TR/wsdl20-primer/

[38]   Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, W3C Recommendation, 26 June 2007.
http://www.w3.org/TR/wsdl20/

[39]   Web Services Description Requirements, W3C Working Draft, 28 October 2002.
http://www.w3.org/TR/2002/WD-ws-desc-reqs-20021028/

[40]   Web Services Glossary, W3C Working Draft, 14 November 2002.
http://www.w3.org/TR/2002/WD-ws-gloss-20021114/

[41]   XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2004.
http://www.w3.org/TR/xmlschema-2/

3 DEFINITIONS

3.1 Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [28]. These key words are capitalized when used to unambiguously specify requirements. When these words are not capitalized, they are meant in their natural-language sense.

All examples in the document are labeled as "non-normative", which means they are not to provide a canonical implementation for use in a registry or artifact, but merely to illustrate technical features of a particular approach.

3.2 Terms and Definitions

Access Control	Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities. [29]
Asynchronous Operation	A type of operation whose message exchange pattern allows messages to be sent without precise sequencing, e.g., a flow of sensor event messages which need not be individually acknowledged. [40]
Attribute-Based Access Control (ABAC)	A process in which access to system resources is granted to a user based on the value of a user's attributes. While user authentication is still required, the access is no longer granted via a specific access control list.
Audit	A process that records information needed to establish accountability for system events and for the actions of system entities that cause them. [29]
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities. [29]
Authentication	The process of verifying an identity claimed by or for a system entity. [29]
Authorization	The granting of rights or permission to a system entity (mainly but not always a user or a group of users) to access a Web service.
Binding	An association between an interface, a concrete protocol, and a data format. A binding specifies the protocol and data format to be used in transmitting messages defined by the associated interface. [39]
Business Function	A characteristic action or activity that needs to be performed to achieve a desired objective, or in the context of this standard, to achieve a real world effect. (Adapted from [14])
Confidentiality	Protective measures that assure that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity). [29]

Credentials	Data that is transferred to establish the claimed identity of an entity. [22]
Critical Failure	A state or condition in which a service is unable to perform the primary function for which it was designed.
Data Element	A unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes. [19]
Datatype	A computer representation of a well-known abstract concept such as *integer* or *date*. [41]
Description	An account of the content of a resource. (Adapted from [17])
Discovery	The processes through which a service consumer may search for and find services, (generally done by providing criteria to search for against a corpus of service metadata which service providers have provided to describe their services). [10]
Effect	A state or condition that results from interaction with a service. Multiple states may result depending on the extent to which the interaction completes successfully or generates a fault. [10]
FAA Data Registry (FDR)	The official source of the FAA's data standards. The FDR (http://fdr.gov/fdr/Home.jsp) is a Web-enabled system that provides ready access to the agency's standards and is compliant with the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Standard 11179, Information Technology – Metadata Registries (MDR), Parts 1 – 6 (http://metadata-standards.org/11179/). [3]
FAA-Affiliated Registry	An FAA registry that implements sharing of information with other registries within the FAA. [9]
Fault	A message that is returned as a result of an error that prevents a service from implementing a required function. A fault usually contains information about the cause of the error.
Format	The arrangement of bits or characters within a group, such as a data element, message, or language.
Hyperlink	In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by color or underscoring) that points (indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link. [24]
Idempotent	A term used to describe an operation in which a given message will have the same effect whether it is received once or multiple times; i.e., receiving duplicates of a given message will not cause any undesirable effect.
Identifier (ID)	A sequence of characters, capable of uniquely identifying that with which it is associated, within a specified context. [19]

Input Data entered into, or the process of entering data into, an information processing system or any of its parts for storage or processing. (Adapted from [23])

Integrity Protective measures that assure that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [29]

Interface See Service Interface.

Internet A large, heterogeneous collection of interconnected systems that can be used for communications of many different types between any interested parties connected to it. The term includes both the "core Internet" (Internet service provider networks) and "edge Internet" (corporate and private networks, often connected via firewalls, network address translation boxes, application layer gateways, and similar devices). [31]

Interoperability The ability of software and hardware on multiple machines from multiple vendors to communicate. [18]

Loose-Coupling A characteristic of software systems, in which dependencies among a system's constituting parts have been minimized. [33]

Message An identifiable collection of units of information (data elements), presented in a manner suitable for communication, interpretation, or processing within a context of interacting SOA components.

Message Exchange Pattern (MEP) A template, devoid of application semantics, that describes a generic pattern for the exchange of messages between agents. It describes the relationships (e.g., temporal, causal, sequential, etc.) of multiple messages exchanged in conformance with the pattern, as well as the normal and abnormal termination of any message exchange conforming to the pattern. [40]

Metadata Data that defines or describes other data. [19]

Name The designation of an object by a linguistic expression. [19]

Namespace A collection of names, identified by a URI reference, that are used in XML documents as element types and attribute names. The use of XML namespaces to uniquely identify metadata terms allows those terms to be unambiguously used across applications, promoting the possibility of shared semantics. [17]

Net-Centricity The realization of a networked environment, including infrastructure, systems, processes, and people.

Non-Repudiation Protective measures against false denial of involvement in a communication. [29]

Normative Document	A document that provides rules, guidelines, or characteristics for activities or their results. Note: The term "normative document" is a generic term that covers such documents as standards, technical specifications, codes of practice, and regulations. [23] In the context of this standard, a normative document is a set of rules that (1) determines the behavior of interacting entities and (2) has been developed by a recognized body in industry or academia and established by consensus in the FAA.
Operation	A set of messages related to a single Web service action. [39]
Organization	A unique framework of authority within which a person or persons act, or are designated to act, towards some purpose. Any department, service, or other entity within an organization which needs to be identified for information exchange. [21]
Output	Data transferred out of, or the process by which an information processing system or any of its parts transfers data out of, that system or part. (Adapted from [23])
Overload	A condition where the workload exceeds the resources available.
Permissible Values	The set of allowable instances of a data element.
Policy-Based Access Control (PBAC)	A process in which access to system resources is defined and enforced centrally according to formal government policy, and not by local administrators.
Precondition	A state or condition that is required to be true before an action can be successfully invoked. [10]
Processing	A set of algorithms, calculations, or business rules that operate on input data in order to produce the required output or to produce a change of internal state.
Protocol	A formal set of conventions governing the format and control of interaction among communicating functional units. [13]
Quality of Service (QoS) Characteristic	A parameter that specifies and measures the value of a provided service. [10]
Real World Effect	An ultimate purpose associated with the interaction with a particular service. It may be the response to a request for information or the change in the state of some entities shared between the participants in the interaction. (Adapted from [26])
Registry	An enabling infrastructure that uses a formal registration process to store, catalog, and manage metadata relevant to a service. A registry supports the search, identification, and understanding of resources, as well as query capabilities. [9]

Requester Agent	A [software agent](#) that is designed to interact with a [Web service](#) in order to request that a task be performed on behalf of its owner – the [service consumer](#). (Adapted from [10])
Resource	An object of information that is available on an [Internet](#) and identified by a unique [Uniform Resource Identifier](#). [9]
Role	A collection of permissions to use [resources](#) made available by a [Web service](#).
Role-Based Access Control (RBAC)	A form of identity-based [access control](#) where the system entities that are identified and controlled are functional positions in an [organization](#) or process. [10]
Security	The protection of information and data so that unauthorized persons or systems cannot read or modify them and [authorized](#) persons or systems are not denied access to them. [20]
Semantics	A conceptualization of the implied meaning of information that requires words and/or symbols within a usage context. [25]
Service	See [Web service](#).
Service Category	One or more values selected from a hierarchical convention that is used to categorize all FAA [services](#). [11]
Service Consumer	An [organization](#) that seeks to satisfy a particular need through the use of capabilities offered by means of a [service](#). (Adapted from [25])
Service Criticality	A single value selected from a list of values that is used to categorize a [service](#) in terms of the significance given to a functional failure of that service. [11]
Service Description	The information needed in order to use, or consider using, a [service](#). (Adapted from [25])
Service Interface	An abstract boundary that a [Web service](#) exposes. It defines the types of [messages](#) and the [message exchange patterns](#) that are involved in interacting with the Web service, together with any conditions implied by those messages. [36]
Service Provider	An [organization](#) that offers the use of capabilities by means of a [service](#). (Adapted from [25])
Service-Oriented Architecture (SOA)	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. A SOA provides a uniform means to offer, [discover](#), interact with, and use capabilities to produce desired [effects](#) consistent with measurable [preconditions](#) and expectations. [10]

Software Agent   A running program that drives Web services, both to implement them and to access them. [36]

Standard   A document established by consensus and approved by a recognized body, which provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: standards should be based on the consolidated results of science, technology, and experience, and aimed at the promotion of optimum community benefits. [23]

Structured Data   Data that is organized in well-defined semantic "chunks" or units that are variously called fields, elements, objects, or entities. Individual units are often combined to form larger, more complex units. (Adapted from [6])

Synchronous Operation   A type of operation whose message exchange pattern describes temporally coupled or "lock-step" interactions, e.g., remote procedure call (RPC)-style request-response interactions. [40]

Taxonomy   A system or controlled list of values by which to categorize or classify objects. [11]

Token   A data object or a portable, user-controlled, physical device used to verify an identity in an authentication process. [29]

Uniform Resource Identifier (URI)   A compact string of characters for identifying an abstract or physical resource. [32]

Uniform Resource Locator (URL)   A type of URI that identifies a resource via a representation of its primary access mechanism (e.g., its network "location"), rather than by some other attributes it may have. [32]

Unstructured Data   Data that does not follow any hierarchical sequence or any relational rules. Examples of unstructured data may include audio, video, and unstructured text such as the body of an e-mail or word processor document. (Adapted from [6])

User   A human, his/her agent, a surrogate, or an entity that interacts with information processing systems. [23] A person, organization entity, or automated process that accesses a system, whether authorized to do so or not. [24]

Web Service   A platform-independent, loosely-coupled software component designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format. Other systems interact with the Web service in a manner prescribed by its description by means of XML-based messages conveyed using Internet transport protocols in conjunction with other Web-related standards. (Adapted from [40])

3.3 Acronyms and Abbreviations

ABAC   Attribute-Based Access Control

AIM   Aeronautical Information Management

AIXM   Aeronautical Information Exchange Model

CMS   U.S. Department of Health and Human Services Centers for Medicare and Medicaid

DCMI   Dublin Core Metadata Initiative

DOT   Department of Transportation

FAA   Federal Aviation Administration

FDR   FAA Data Registry

FTP   File Transfer Protocol

GML   Geography Markup Language

HTTP(S)   Hypertext Transfer Protocol (Secure)

ID   Identifier

IETF   Internet Engineering Task Force

IRD   Interface Requirements Document

ISO/IEC   International Organization for Standardization/International Electrotechnical Commission

IT   Information Technology

Java EE   Oracle Java Platform, Enterprise Edition

JMS   Java Message Service

MDR   Metadata Registry

MEP   Message Exchange Pattern

MS .NET   Microsoft .NET Framework

MS DCOM   Microsoft Distributed Component Object Model

MTBCF   Mean Time Between Critical Failure

MTBF	Mean Time Between Failure
MTTR	Mean Time To Restore
NAS	National Airspace System
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OMG CORBA	Object Management Group Common Object Request Broker Architecture
PBAC	Policy-Based Access Control
PIN	Personal Identification Number
PNG	Portable Network Graphics
QoS	Quality of Service
RBAC	Role-Based Access Control
REST	Representational State Transfer
RFC	Request For Comment
RPC	Remote Procedure Call
SEM	System Engineering Manual
SOA	Service-Oriented Architecture
SOAP	Originally "Simple Object Access Protocol"; the full spelling is no longer used
Sun Jini	Sun Microsystems Jini Technology
SVG	Scalable Vector Graphics
TCP/IP	Transmission Control Protocol/Internet Protocol
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VRTM	Verification Requirements Traceability Matrix
W3C	World Wide Web Consortium
WS	Web Service

WSDD   Web Service Description Document

WSDL   Web Service Description Language

WSRD   Web Service Requirements Document

XML   eXtensible Markup Language

4 GENERAL REQUIREMENTS

This section describes requirements for the stylistic aspects of the WSRD. Detailed requirements for the structure and content of the WSRD are provided in section 5.

4.1 Text, Grammar and Style

a. The text SHALL be written in clear and simple language, free of vague terms, or those subject to misinterpretation.

b. All sentences SHOULD be complete and grammatically correct. Refer to FAA Order 1000.36, FAA Writing Standards [1] for guidance.

c. The United States Government Printing Office Style Manual [16] SHALL be used as a guide for capitalization, spelling, punctuation, syllabification, compounding words, tabular work, and other elements of grammar and style.

4.2 Key Terms

a. Requirements levied in the WSRD SHALL be expressed using the terms "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", or "OPTIONAL" to specify requirements.

b. These terms SHALL be interpreted as described in RFC 2119 [28].

c. These terms SHALL be capitalized when used to unambiguously specify requirements.

4.3 Page Numbering

a. The front cover page SHALL omit the page number.

b. All pages after the front cover page and before the page containing the first ("Scope") section SHALL be numbered consecutively with lower-case Roman numerals, starting with ii (for example, ii, iii, and iv).

c. The first page of the first ("Scope") section SHALL be numbered with an Arabic numeral 1.

d. All subsequent pages SHALL be numbered sequentially using Arabic numerals.

e. The page numbers SHALL be placed at the bottom center of each page.

4.4 Page Headers

a. Each page, including the front cover, SHALL contain a header in the upper right-hand corner right-justified.

b. Each header SHALL contain the WSRD Identifier. Note: In most cases, the identifier is assigned by a governing or configuration management organization under whose authority the service is developed or functions.

c. If the WSRD is a revision to a baselined WSRD, the word "Revision" followed by the revision letter SHALL be included immediately under the WSRD Identifier.

d. If the WSRD has been approved by a governing or configuration management control organization, the header SHALL include the date of WSRD approval on the last line.

e. If the WSRD is a draft, the header SHALL include the word "DRAFT" in capital letters under the WSRD identifier and the date of the draft on the next line.

4.5 Use of Hyperlinks

To improve the readability and understanding of the WSRD, usage of hyperlinks is prescribed as follows:

a. Every term that is used and defined within the WSRD SHOULD be linked via a hyperlink reference to the location of its definition in the WSRD's "Definitions" section.

b. When the same term is used more than once within the same sentence or paragraph, only the first occurrence of the term SHOULD be referenced.

c. Every document that is cited within the WSRD SHALL be linked via a hyperlink reference to the location of its bibliographic entry in the WSRD's "Applicable Documents" section.

d. When a document is quoted within the WSRD, the quote SHALL include a hyperlink reference to the location of the document's bibliographic entry in the WSRD's "Applicable Documents" section.

4.6 Use of Diagrams

There are a number of sections in the WSRD where using diagrams is suggested to enhance the understanding of a described topic.

a. Unified Modeling Language (UML) diagrams are RECOMMENDED since UML is able to concisely describe concepts without implying any specific technology. Information about UML diagrams is available at http://www.uml.org/.

4.7 Identifying Figures, Tables, and Appendices

a. Figures SHALL be identified by "Figure", the level one section number in which they appear followed by a dash and numbered sequentially using Arabic numerals within the level one section (e.g., 3-1, 3-2, 3-3, 4-1, 4-2), followed by the figure title.

b. The figure identification SHALL be placed below the figure.

c. Tables SHALL be identified by "Table", the level one section number in which they appear followed by a dash and numbered sequentially using Arabic numerals within the level one section (e.g., 3-1, 3-2, 3-3, 4-1, 4-2), followed by the table title.

d. The table identification SHALL be placed above the table.

e. Appendices SHALL be identified by "Appendix", followed by sequential capital letters (e.g., Appendix A), and the appendix title.

5 DETAILED REQUIREMENTS

This section describes requirements for the structure and content of the WSRD.

5.1 Cover Page

a. The WSRD SHALL include a cover page as the first page.

b. The upper left corner of the cover page SHALL include the FAA signature (the Department of Transportation triskelion figure with the words "U.S. Department of Transportation" and the words "Federal Aviation Administration" below it) in accordance with FAA Order 1700.6, FAA Branding Policy [4].

c. The line "Web Service Requirements Document" SHALL be centered above the title.

d. The title SHALL be the name by which the service will be known. Note: In most cases, the title will consist of the approved service's name issued by the activity authorized to assign the name. That name will be referred to throughout the WSRD as the Web service name.

An example of a WSRD cover page is shown in Appendix A.

5.2 Approval Page (Optional)

Signatures on this page ensure that the interested parties have approved the WSRD content. The approval page may not be required based on the configuration management policies established within a given organization. The following statements apply when signed approval is required.

a. The approval page SHALL be the first interior page of the WSRD.

b. The approval page SHALL contain the line "Web Service Requirements Document" centered above the title of the Web service, and the line "Approval Signatures" centered below the title of the Web service.

c. The approval page SHALL include information for every cosigner.

d. The information SHALL include the cosigner's full name.

e. The information SHALL include the full name of the cosigner's organization followed by the acronym by which the organization is commonly recognized within FAA.

f. The information SHALL include the cosigner's signature.

g. The information SHALL include the date of the signature.

An example of a WSRD Approval Page is shown in Appendix B.

5.3 Revision Record Page

a. The WSRD SHALL include a revision record page.

b. The revision record page SHALL contain the centered line "Revision Record" above the revision record table.

c. Only revisions SHALL be listed.

d. The revision record page SHALL include information for every revision listed.

e. The information SHALL include the revision letter.

f. The information SHALL include a brief description of the revision.

g. The information SHALL include the date of the revision.

h. The information SHALL include the full <u>name</u> of the person who entered this revision record ("Entered by").

An example of a WSRD Revision Record Page is shown in <u>Appendix C</u>.

5.4 Table of Contents

a. The <u>WSRD</u> SHALL include a table of contents.

b. The WSRD SHALL conform to the basic outline shown in Table I below. Note: the sections shown in italics are optional.

TABLE I. WSRD table of contents

<u>Cover Page</u>
<u>Approval Page</u>
<u>Revision Record Page</u>
<u>Table of Contents</u>
List of Figures
List of Tables
1 <u>Scope</u>
1.1 Background
2 <u>Applicable Documents</u>
2.1 Government Documents
2.2 Non-Government Standards and Other Publications
3 <u>Definitions</u>
3.1 Terms and Definitions
3.2 Acronyms and Abbreviations
4. <u>Required Service Information</u>
4.1 <u>Service Characteristics</u>
4.2 <u>Service Provider</u>
4.3 <u>Service Consumers</u>
5 <u>Functional Requirements</u>
5.1 <u>Service Business Function Requirements</u>
5.2 <u>Service Interface Requirements</u>
5.2.1 <u>Operations</u>
5.2.2 <u>Messages</u>
5.2.3 <u>Faults</u>
5.2.4 <u>Data Elements</u>
5.3 <u>Machine-Processable Service Description Document</u>
6 <u>Non-Functional Requirements</u>

5.5 Scope

a. Section 1 of the WSRD SHALL provide a scope statement that briefly describes the coverage of the WSRD.

b. At a minimum, section 1 of the WSRD SHALL contain the following sentences: "This WSRD provides the requirements for the [name of the Web service]. It has been prepared in accordance with FAA-STD-070, Department of Transportation Federal Aviation Administration, *Preparation of Web Service Requirements Documents* [*cite reference or hyperlink*]."

c. The name of the Web service SHALL be identical with the name of the Web service provided on the cover page of the WSRD.

d. Section 1 of the WSRD MAY include paragraphs on the WSRD's purpose, applicability, background, etc. as needed to give readers of the WSRD a context for understanding the body of the WSRD.

e. Section 1 of the WSRD SHALL NOT contain requirements.

5.6 Applicable Documents

a. Section 2 of the WSRD SHALL list all documents specifically cited in the WSRD.

b. Only documents that are specifically cited in the WSRD SHALL be listed in section 2.

c. Every document listed in section 2 of the WSRD SHALL be described through a common set of metadata attributes, as shown below:

   1. The metadata SHALL include the full title of the document.

   2. The metadata SHOULD include the alternate title or abbreviated name by which the document is known or recognized. This is particularly relevant for normative documents.

   3. The metadata SHALL include the publisher of the document.

   4. The metadata SHALL include the publication date of the document.

   5. The metadata SHOULD include the appropriate version of the document (e.g., the latest version, the version needed for compatibility with other documents, the version of the document that is under contract by the project.)

   6. The metadata SHOULD include the creator of the document, if it is different from the publisher.

   7. The metadata SHALL include the address or location (preferably network location, i.e., URL) where a copy of the document can be obtained.

d. Section 2.1 of the WSRD SHALL list all types of Government standards and other publications cited in the WSRD.

e. Section 2.2 of the WSRD SHALL list all types of non-Government standards and other publications cited in the WSRD.

f. When requirements are contained in a referenced document, the WSRD SHALL specify the extent of the applicability of the referenced requirements (i.e., the section(s) or paragraph(s) that are applicable) if the whole document is not applicable.

g. When requirements are contained in a referenced document, the WSRD SHALL specify the extent of any tailoring of those requirements.

h. Applicable documents MAY also be used in the WSRD to provide information or clarification without imposing requirements.

i. When a document is quoted within the WSRD, the quote SHOULD indicate where in the document the quote is to be found (e.g., using section number, paragraph number, page number, or other means of identification).

5.7 Definitions

a. Section 3.1 of the WSRD SHALL define all terms used in the WSRD to provide for clarity, unless the terminology is generally accepted and not subject to misinterpretation.

b. Only terms that are specifically used in the WSRD SHALL be listed in section 3.1.

c. Definitions MAY be included by reference to another document.

d. Terms and their definitions SHALL be listed in alphabetical order.

e. At a minimum, section 3.1 of the WSRD SHALL contain the following paragraph: "The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [*cite reference or hyperlink, i.e.,* http://www.rfc-editor.org/rfc/rfc2119.txt]. These keywords are capitalized when used to unambiguously specify requirements. When these words are not capitalized, they are meant in their natural-language sense."

f. Section 3.2 of the WSRD SHALL include a list of acronyms and abbreviations used in the WSRD, together with their full spelling.

g. Only acronyms and abbreviations that are specifically used in the WSRD SHALL be listed in section 3.2.

h. Acronyms and abbreviations SHALL be listed in alphabetical order.

5.8 Required Service Information

Section 4 of the WSRD provides required information and metadata about the service characteristics, the service provider, and the service consumers.

a. Section 4 of the WSRD SHALL NOT contain requirements.

5.8.1 Service Characteristics

a. Section 4.1 of the WSRD SHALL specify information about the service characteristics that are important for (1) gaining a proper understanding of the business objectives of the service as a part of its operational environment and (2) supporting semantic consistency in service registration and future service description.

b. The information SHALL include the name of the service.

c. The name SHALL be identical with the name of the service provided on the cover page of the WSRD.

d. The information SHALL include a brief plain language description of the service. Note: That description is similar to or the same as the description to be used to register this service in an FAA-affiliated registry. For more details, see FAA-STD-064, Web Service Registration [9].

e. The information SHALL include a service namespace. See FAA-STD-063, XML Namespaces [8] for establishing a namespace.

f. The information SHALL include a service revision letter consistent with section 5.3 requirement (e) of this standard.

g. The information SHALL include a service category.

h. One or more values representing the service category SHALL be selected from the FAA Service Category Taxonomy described in section 5.3.5 of FAA-STD-066, Web Services Taxonomies [11].

i. The information SHALL include the level of criticality for the service.

j. The single value representing the service's criticality level SHALL be selected from the Service Criticality Taxonomy described in section 5.3.8 of FAA-STD-066 [11].

k. The information MAY include additional service characteristics; e.g., classifications using business domain-specific taxonomies.

5.8.2 Service Provider

a. Section 4.2 of the WSRD SHALL specify information about the service provider, that is, the FAA organization ultimately responsible for service development and future operation.

b. The information SHALL include the name of the service provider organization.

c. The name SHALL consist of the full name spelled out followed by the acronym by which it is commonly recognized within FAA.

d. The information SHALL include a brief plain language description of the organization. Note: That description is similar to or the same as the description to be used to register this organization in an FAA-affiliated registry. For more details, see FAA-STD-064, Web Service Registration [9].

e. The information SHALL include an organization namespace. See FAA-STD-063, XML Namespaces [8] for establishing a namespace.

f. The information MAY include an accessible reference (e.g., URL) to the Web page that supplies information about the organization.

5.8.3 Service Consumers

a. Section 4.3 of the WSRD SHALL specify information about consumers that are expected to use the service.

b. The information MAY include each known consumer organization's full name (and acronym if applicable).

c. The information MAY include a brief plain language description of each known organization. Note: That description is similar to or the same as the description to be used to register this organization in an FAA-affiliated registry. For more details, see FAA-STD-064, Web Service Registration [9].

d. The information MAY include an accessible reference (e.g., URL) to the Web page that supplies information about each known organization.

5.9 Functional Requirements

Section 5 of the WSRD specifies requirements for the business functions that the service must be able to perform and the interface between the service and its consumers.

5.9.1 Service Business Function Requirements

Section 5.1 of the WSRD addresses requirements for service functions from a business point of view, that is, from the point of view of consumer organizations that will use the service to conduct their business. Such requirements do not deal with the mechanics of interacting with a service (this aspect is addressed in the Service Interface section), but rather with what activities need to be performed in order to achieve a "real world effect" or specific purpose associated with interacting with the service. For example, a real world effect could be that a flight was rerouted, weather information was received, etc. Requirements in this section are written with emphasis on the functionality of the entire service and not on the specific operations, which are addressed in section 5.2.1 of the WSRD.

  a. Section 5.1 of the WSRD SHALL specify requirements for the service business functions.

  b. If the service business functions have also been described in architectural or other requirements documents, the requirements SHOULD contain specific references to these documents.

5.9.2 Service Interface Requirements

Section 5.2 of the WSRD specifies requirements for the service interface. This section also includes requirements for operations, messages, faults, and data elements associated with the interface.

  a. Section 5.2 of the WSRD SHALL specify requirements for the interface implemented by the Web service.

  b. The interface specification SHALL provide a name that uniquely identifies the interface throughout the WSRD.

  c. The interface specification SHALL provide a plain language description of the interface.

  d. The interface specification SHALL provide a list of names of all the operations that are implemented by the interface.

  e. All operations that constitute the interface SHALL be defined in section 5.2.1 of the WSRD as prescribed in section 5.9.2.1 of this standard.

It is possible, although rarely recommended, that a service may have more than one interface.

  f. When a service exposes multiple interfaces, each interface SHALL be specified in section 5.2 of the WSRD as described above in requirements (a) through (e).

5.9.2.1 Operations

Section 5.2.1 of the WSRD specifies the requirements for the operations that will be offered by the Web service. Every operation that is listed in WSRD section 5.2.1 Operations represents the patterns and content of interactions of messages described in WSRD section 5.2.2 Messages.

  a. Section 5.2.1 of the WSRD SHALL specify every operation that is a part of the interface described in section 5.2 of the WSRD.

  b. Each operation specification SHALL provide a name that uniquely identifies the operation throughout the WSRD.

  c. Each operation specification SHALL provide a plain language description of the operation. For example, "allows consumer to retrieve current status of a specified flight."

d. Each operation specification SHALL indicate the <u>Message Exchange Pattern</u> (MEP) that is implemented by the operation by using a single value selected from the Message Exchange Pattern <u>Taxonomy</u> described in section 5.3.11 of FAA-STD-066 <u>[11]</u>.

e. Each operation specification SHALL provide the type of the operation by indicating whether it is "<u>synchronous</u>" or "<u>asynchronous</u>".

f. Each operation specification SHALL state if the operation is <u>idempotent</u> or non-idempotent.

g. Each operation specification SHALL describe a <u>precondition</u>, that is, a description of the state or condition that should be true before the operation can proceed. A typical example is, "the user has logged in and has been authenticated and authorized to access the service."

h. Each operation specification SHALL describe an <u>input</u>, that is, the information that initiates interaction, including the name of the relevant input message defined in section 5.2.2 of the WSRD.

i. Each operation specification SHALL describe an <u>output</u>, that is, the information that is produced in response to a request, including the name of the relevant output message defined in section 5.2.2 of the WSRD.

j. Each operation specification SHALL describe an <u>effect</u>, that is, a description of the state or condition that exists after the operation is completed (assuming that no error has occurred). For example, "requested map was generated and returned to a consumer."

k. Each operation specification SHALL describe the <u>fault</u>(s), that is, the information that is produced in response to conditions that result in operation failure, including the name of the corresponding fault message defined in section 5.2.3 of the WSRD.

l. All messages referenced in requirements for service operations SHALL be defined in section 5.2.2 of the WSRD as prescribed in <u>section 5.9.2.2</u> of this standard.

m. All faults referenced in requirements for service operations SHALL be defined in section 5.2.3 of the WSRD as prescribed in <u>section 5.9.2.3</u> of this standard.

n. Section 5.2.1 of the WSRD SHOULD include a diagram that shows how and in what order messages are exchanged within the context of the operation.

5.9.2.2 Messages

a. Section 5.2.2 of the <u>WSRD</u> SHALL specify all <u>input</u> and <u>output</u> <u>messages</u> that are exchanged between the <u>service</u> and a <u>requester agent</u>. (Note: <u>fault</u> messages are specified separately as described in <u>section 5.9.2.3</u> below.)

b. Each message specification SHALL provide a <u>name</u> that uniquely identifies the message throughout the WSRD.

c. Each message specification SHALL provide a plain language <u>description</u> of the message.

d. Each message specification SHALL specify a message direction that indicates whether the message is coming to the service ("in") or going from the service ("out").

e. Each message specification SHALL provide a list of all <u>data elements</u> and/or data objects that comprise the message.

f. All data elements referenced in section 5.2.2 of the WSRD SHALL be defined in section 5.2.4 of the WSRD as prescribed in <u>section 5.9.2.4</u> of this standard.

5.9.2.3 Faults

This section describes requirements for the faults to be generated in response to conditions that result in failure of an operation or set of operations.

    a. Section 5.2.3 of the WSRD SHALL specify all faults.

    b. Each fault specification SHALL provide a name that uniquely identifies the fault throughout the WSRD.

    c. Each fault specification SHALL provide a plain language explanation of the cause of the fault.

    d. Each fault specification MAY provide a fault originator. For example, the fault originator might be a database to which the service passes information received from a consumer that prompts an error.

    e. Each fault specification MAY describe an underlying cause that resulted in this fault. Note: there could be an unlimited number of causes.

    f. Section 5.2.3 of the WSRD SHOULD include requirements for information and/or data elements (e.g., fault code, timestamp, etc.) to be provided with every fault message returned by a service which are not addressed above in requirements **b** through **e**.

    g. All data elements referenced in section 5.2.3 of the WSRD SHALL be defined in section 5.2.4 of the WSRD as prescribed in section 5.9.2.4 of this standard.

5.9.2.4 Data Elements

Section 5.2.4 of the WSRD specifies all data elements that will appear in messages (or faults) to be sent or received by the Web service.

A data element is "a unit of data for which the definition, identification, representation and permissible values are specified by means of a set of attributes." [19]

- *Definition* provides the knowledge of what it is or what it means so it can be understood and used correctly.

- *Identification* provides a means for referring to it, recognizing it, or distinguishing it from all other elements.

- *Representation* describes how it is portrayed or depicted (format, datatype, language, etc.) so it can be interpreted.

- *Permissible values* provide the set or range of its possible instances (values).

In addition, a data element always exists (has meaning) in the context of some *information model* or schema that defines the element in terms of its relationships with other elements. A full understanding of a data element cannot be achieved without the presence of such a model.

A data element can be *complex*, that is, contain other data elements (e.g., an element Address composed of Street Address, City, State, and Postal Code elements), or it can be *primitive* (i.e., indivisible). Either kind is specified with the same set of attributes.

Note: requirements (a) through (s) specified below are applicable only to structured data, that is, data that conforms to a data model and/or identifiable formal structure of logical components or compound objects. Structured data is usually stored in databases and in a Web services environment is rendered as XML documents. Unstructured data (e.g., image, audio, or binary-encoded data) is addressed in requirements (t) and (u) below.

a. Section 5.2.4 of the WSRD SHALL list and specify all data elements, complex or primitive, that appear in messages (or faults) to be sent or received via the Web service.

b. Each element specification SHALL provide a namespace for the element. Note: if all elements in the list are defined in the same namespace, the namespace can be indicated once for the whole list. Note: See FAA-STD-063 [8] for establishing a namespace.

c. Each element specification SHALL provide a name that uniquely identifies the element within its namespace.

d. For elements that are registered in the FAA Data Registry (FDR), the specification SHALL provide the FDR registration identifier. Note: See FAA-STD-060 [7] for information about registering data elements in FDR.

e. Each element specification SHALL provide a plain language definition of the element.

f. Each element specification SHALL provide a description of the element's permissible values in one of the following forms: a range of numbers, a list of individual values, a reference to a source that lists the values (e.g., "FAA Order 7350.7 Location Identifiers"), or a textual description (e.g., "Not Applicable").

g. For elements whose values represent codes, the element specification SHALL provide the meanings of the codes (e.g., "BR = Mist, VA = Volcanic Ash, DU = Widespread Dust, etc.").

h. For elements whose values represent quantitative measures, the element specification SHALL provide the unit of measure (e.g., feet, kilograms, degrees Fahrenheit, dollars).

i. Each element specification SHALL provide the element's datatype.

j. For primitive elements, the element specification SHALL denote datatype using the typing system defined in section 2 of the W3C XML Schema Datatypes specification [41].

k. For complex elements, the element specification SHALL denote datatype as "complex".

l. Each element specification MAY provide the element's maximum length together with units of length (e.g., characters, bytes, etc.), if applicable.

m. If an element is to be rendered in a special format, the element specification SHOULD provide a format string.

n. Regular expressions as defined in Appendix F of the W3C XML Schema Datatypes specification [41] are RECOMMENDED for use in describing formats.

o. Each element specification SHALL provide the obligation ("Required" or "Optional") of the element, i.e., whether the element is required or optional in the context of its underlying information model.

p. Each element specification SHALL provide the multiplicity (occurrence) of the element in the context of its underlying information model (e.g., 0,1,...,unbounded).

q. Each element specification SHALL provide the information described above in requirements (b) through (d) even if the information is already contained in another document (e.g., an XML schema file), or artifact.

r. If there are documents or artifacts that contain the information described above in requirements (e) through (p), the element specification MAY provide accessible references (e.g., URL) to these documents or artifacts in lieu of providing the information itself.

s. Section 5.2.4 of the WSRD SHALL include a diagram, or an accessible reference (e.g., URL) to a document or artifact containing such a diagram, that depicts a conceptual or logical model of the data elements listed.

t. If the data that appears in messages is unstructured, section 5.2.4 of the WSRD SHALL specify the type, format, and plain language description of the data.

u. If the data that appears in messages is unstructured, section 5.2.4 of the WSRD SHALL refer to section 7.1.1.1 (or 7.1.n.1, as appropriate) of the WSRD that describes how the data should be encoded (see also section 5.11.1.1 of this standard).

5.9.3 Machine-Processable Service Description Document

As stated in section 1.3.2 of this standard, Web services are self-describing; that is, a service should be presented with an externalized and accessible service description that defines and describes its interface and invocation bindings. To support direct interaction with service consumers, this description is realized as a document rendered in a machine-processable format via a common XML grammar.

While the Web Service Description Language (WSDL) specification set forth by W3C provides the most popular format for developing machine-processable descriptions of Web services (because of this popularity, a machine-processable service description is commonly referred to as a "WSDL file"), there are other formats that are used in industry and in the FAA (e.g., the XML Capabilities document defined by the OGC).

For the purpose of this standard, we assert that a machine-processable service description document is: 1) an integral part of the Web service, 2) a sub-product of development of the Web service, 3) developed as part of the development of the Web service, and 4) specified by requirements established in the Web service's WSRD.

Note: the machine-processable service description document described in this section should not be confused with the human-readable Web Service Description Document (WSDD) defined in FAA-STD-065 [10]. The requirements for developing a WSDD are usually regulated by system engineering or configuration management bodies of service provider organizations and are outside the scope of this standard.

a. Section 5.3 of the WSRD SHALL specify requirements for development of the machine-processable service description document.

b. Section 5.3. of the WSRD SHALL specify the normative document that regulates the format for the machine-processable service description document.

c. The normative document SHALL be specified as prescribed in section 5.6 of this standard.

d. If an accessible reference (e.g., URL) to the normative document is not available, the document itself SHALL be included in an Appendix of the WSRD.

e. Section 5.3 of the WSRD SHALL specify the point in the service's development schedule at which the machine-processable service description document is to be developed (e.g., prior to development or when development is concluded).

5.10 Non-Functional Requirements

Section 6 of the WSRD specifies requirements for properties that exhibit constraints over the functionality of the service.

5.10.1 Quality of Service Requirements

Qualities of Service (QoS) are measurable characteristics that the Web service is expected to meet or possess. These characteristics, or parameters, are documented by specifying a parameter's name, definition, required value or range of values it is expected to meet or possess, the method to be used to measure or calculate its values, and the unit of measure in which its values are expressed. Table II contains a comprehensive but not necessarily complete list of QoS parameters that may be relevant to Web services. The QoS requirements are a combination of performance requirements and information necessary for the developers to size the service software in addition to allowing the service consumers to understand the level of service they can expect.

    a. Section 6.1 of the WSRD SHALL specify requirements to be met by the service for all QoS parameters that are deemed by the WSRD author to be relevant to the service.

    b. Section 6.1 of the WSRD SHALL specify the name, definition, method of calculation, unit of measure, and required value(s) for all QoS parameters listed.

    c. The WSRD author SHOULD select from among, and specify required value(s) for, the QoS parameters provided in Table II.

    d. The definition, method of measurement or calculation, and unit of measure for each QoS parameter specified in section 6.1 of the WSRD SHOULD conform to the definition, method, and unit of measure provided in Table II for the corresponding parameter of that name.

    e. If the QoS parameter being specified has a definition, method, and/or unit of measure different from those of a parameter with the same name in Table II, or if no parameter of that name is listed in Table II, then the definition, method, or unit of measure of the parameter being specified SHALL be provided.

    f. If a QoS parameter is relevant but its required value cannot be determined at this time, a description of how the value will be determined SHALL be specified in place of its required value.

TABLE II. Preferred QoS parameters

QoS Parameter Name	Definition	Method	Unit of Measure	Required Value or Range of Values
Accuracy	Number of errors produced by the service over a period of time.	Simple count. Measurements are taken daily and apply to the preceding 24-hour period.	Whole positive number	
Availability	Probability that the service is present or ready for immediate use.	100 * ((24 – Total Outage Time in Hours) / 24). Measurements are taken daily and apply to the preceding 24-hour period.	Percentage, accurate to 3 decimal places.	
Capacity	Number of service requests that the service can accommodate within a given time period.	Simple count.	Whole positive number, per period of time.	
Mean Time Between Critical Failure (MTBCF)	The average time between hardware or software component failures that result in the loss of the service.	The sum of the individual times between critical failures divided by the number of critical failures.	Hours.	
Mean Time Between Failure (MTBF)	Average time between hardware or software component failures that do not result in the loss of the service.	The sum of the individual times between noncritical failures divided by the number of noncritical failures.	Hours.	
Mean Time To Restore (MTTR)	Average time required to localize a component failure, remove and replace the failed component, and to perform tests to confirm operational readiness of the component.	The sum of the individual times to repair divided by the number of repairs.	Hours.	

QoS Parameter Name	Definition	Method	Unit of Measure	Required Value or Range of Values
Response Time	Maximum time required to complete a service request.	Measured from the time the service provider receives the request to the time the service provider transmits the response.	Seconds.	

5.10.2 Security Requirements

Security is one of the most formidable and unavoidable concerns in the development of both business and mission critical Web services. Web service security is generally understood to be collective measures that enable the service to provide protection against security threats. Security threats to a Web service may include (but are not limited to): unauthorized access to Web service information; unauthorized disclosure, modification and destruction of information; unknown status and repudiation in execution; and denial of service from Web service providers.

Web service security requirements encompass the elements of security for all stages of information exchange and modification, that is, while the data is being processed by a service or while it is in transit between components.

Section 6.2 of the WSRD specifies the requirements for the security measures, procedures, and policies to be implemented by the Web service.

5.10.2.1 Authentication

Authentication is "the process of verifying an identity claimed by or for a system entity" [29] so as to assure that both message sender and message recipient are who they claim to be. Three methods for authentication of Web services are usually deployed: transport layer authentication, token authentication using the WS-Security specification, and SOAP authentication headers.

a. Section 6.2.1 of the WSRD SHALL specify the authentication requirements to be implemented by the Web service.

b. When authentication is implemented by using a standard protocol or specification document, the information about this document SHALL be presented as prescribed in section 5.6 of this standard.

c. When custom implementation of authentication is required, section 6.2.1 of the WSRD SHALL specify requirements for the structure and content of credentials presented to the service.

d. If the WSRD requires the use of a password, then the WSRD SHALL specify the requirements for password complexity and change management in accordance with FAA Order 1370.92A, Password and PIN Management Policy [2].

e. If there are no authentication requirements, section 6.2.1 of the WSRD SHALL include the statement "This WSRD does not impose any authentication requirements."

5.10.2.2 Authorization

In the context of this standard, the authorization process is the granting of rights or permission to a system entity (mainly but not always a user or a group of users) to access a Web service. There are several authorization models, of which the most relevant for SOA are: role-based, attribute-based and policy-based access control. In role-based access control (RBAC), the set of rights and permissions are associated with a particular role, usually corresponding to work functions of an entity. Because RBAC is the most popular authorization model in FAA (it allows for more granular access control and reduces the amount of administrative effort), RBAC specific requirements are included in this section.

    a. Section 6.2.2 of the WSRD SHALL specify the authorization requirements to be implemented by the Web service.

    b. When the RBAC model is deployed, section 6.2.2 of the WSRD SHALL list all roles defined for the Web service.

    c. Every description of a role listed in section 6.2.2 of the WSRD SHALL include the name of the role.

    d. Every description of a role listed in section 6.2.2 of the WSRD SHALL include a description of all rights or permissions associated with that role.

    e. If there are no authorization requirements, section 6.2.2 of the WSRD SHALL include the statement "This WSRD does not impose any authorization requirements."

5.10.2.3 Integrity

In the context of this standard, integrity is understood to be protective measures that assure "that data has not been changed, destroyed, or lost in an unauthorized or accidental manner" [29] either in transit or in storage.

    a. Section 6.2.3 of the WSRD SHALL specify the integrity requirements to be implemented by the Web service.

    b. When integrity is implemented by using a standard protocol or specification document (e.g., XML Signature), the information about this document SHALL be presented as prescribed in section 5.6 of this standard.

    c. If there are no integrity requirements, section 6.2.3 of the WSRD SHALL include the statement "This WSRD does not impose any integrity requirements."

5.10.2.4 Confidentiality

In the context of this standard, confidentiality is understood to be protective measures that assure "that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity)." [29]

    a. Section 6.2.4 of the WSRD SHALL specify the confidentiality requirements to be implemented by the Web service.

    b. When confidentiality is implemented by using a standard protocol or specification document (e.g., XML Encryption), the information about this document SHALL be presented as prescribed in section 5.6 of this standard.

    c. If there are no confidentiality requirements, section 6.2.4 of the WSRD SHALL include the statement "This WSRD does not impose any confidentiality requirements."

5.10.2.5 Non-Repudiation

In the context of this standard, non-repudiation is understood to be protective measures "against false denial of involvement in a communication" [29], that is, assurance that the sender or recipient of a message cannot legitimately claim that they did or did not receive the message. The non-repudiation functionality is often provided through the use of a digital signature or, more typically for SOA, XML Signature.

Note: non-repudiation cannot be established without authentication.

    a. Section 6.2.5 of the WSRD SHALL specify the non-repudiation requirements to be implemented by the Web service.

    b. When non-repudiation is implemented by using a standard protocol or specification document (e.g., WS-Security's standard XML Signature), the information about this document SHALL be presented as prescribed in section 5.6 of this standard.

    c. When an audit capability is required to support non-repudiation, the requirements for audit trail SHALL be described in a separate Audit Capability subsection of the WSRD. See section 5.10.2.6 below.

    d. If there are no non-repudiation requirements, section 6.2.5 of the WSRD SHALL include the statement "This WSRD does not impose any non-repudiation requirements."

5.10.2.6 Audit Capability

In the context of this standard, a security audit is a process that "records information needed to establish accountability for system events and for the actions of system entities that cause them" and an audit trail is "a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities" [29].

    a. Section 6.2.6 of the WSRD SHALL specify the audit requirements to be implemented by the Web service.

    b. Section 6.2.6 of the WSRD SHALL specify the structure and content of the audit trail (e.g., user ID, date, time, event type, security object, success/failure status, etc.).

    c. If there are no audit requirements, section 6.2.6 of the WSRD SHALL include the statement "This WSRD does not impose any audit requirements."

5.10.2.7 Other Security Requirements

It is a common practice for the security functionality of a Web service to be implemented by an intermediary security service, that is, a service that receives a request, performs the security steps, and passes the request to the service provider. (The most typical example of such a service is an XML Gateway.)

    a. When the Web service described in the WSRD will use a separately established security service, section 6.2.7 of the WSRD SHALL provide the name of the security service as well as a brief description of that service and its functionality.

    b. When the Web service described in the WSRD will use a separately established security service, the WSRD SHALL NOT include requirements for that security service.

    c. If there are no other security requirements, section 6.2.7 of the WSRD SHALL include the statement "This WSRD does not impose any other security requirements."
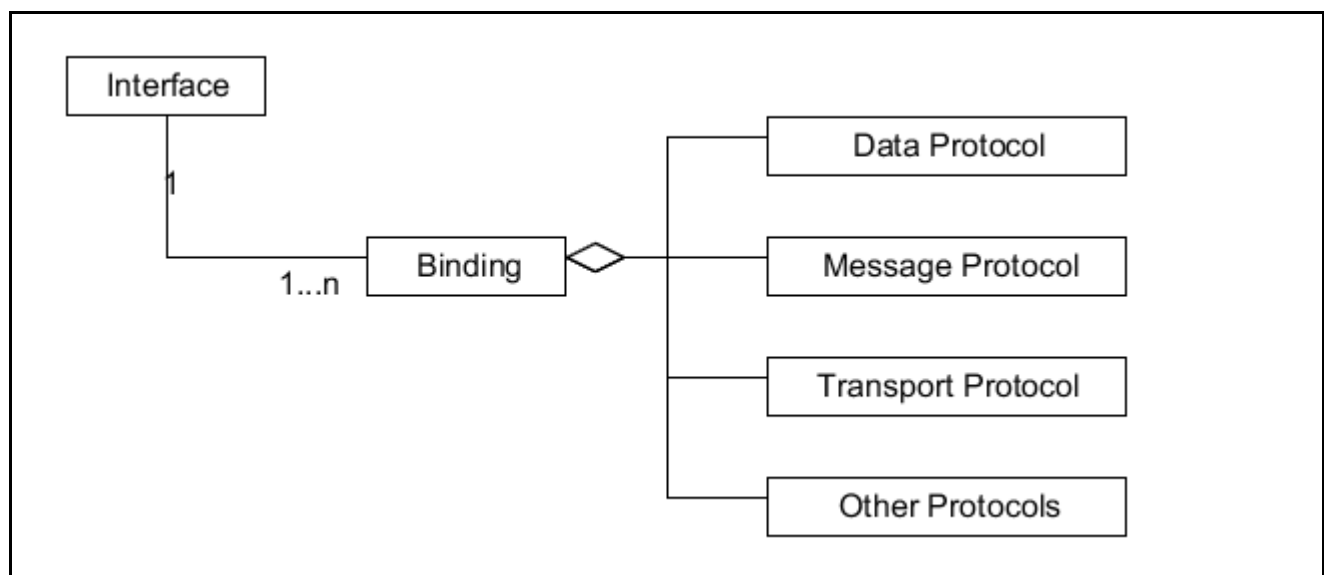
5.11 Implementation Requirements

Section 7 of the WSRD establishes requirements for the means by which the Web service communicates with service consumers. Section 7 also establishes requirements for the operational context of the Web service in terms of the environment and infrastructure within which the service is expected to operate.

5.11.1 Binding Requirements

For the purpose of this standard, a binding is understood to be "an association between an interface, a concrete protocol and a data format. A binding specifies the protocol and data format to be used in transmitting messages defined by the associated interface" [39]. A Web service may offer more than one binding for a single interface, as well as offering different bindings for operations identified as part of that interface. These concepts are illustrated in Figure 3.

FIGURE 3. Binding conceptual diagram

    a. Section 7.1 of the WSRD SHALL specify requirements for all bindings to be implemented by the Web service.

    b. Section 7.1.1 of the WSRD SHALL specify the first binding.

    c. If there are to be multiple bindings, they SHALL be specified in consecutive additional WSRD sections with headings numbered 7.1.2 (or 7.1.n, as appropriate).

    d. The heading of the WSRD section specifying each binding SHALL include the name that will be used throughout the WSRD to refer to that binding.

    e. Each binding specification SHALL include the name of the operation, and the name of an interface associated with this operation, that deploys this binding. Note: when all operations within the interface deploy the same binding, only the interface name is required.

    f. The name of the operation and/or associated interface SHALL be consistent with the

operation and/or interface name established in section 5.2 of the WSRD.

g. Each binding specification SHALL include information about each data protocol that the service uses for this binding, as described in <u>section 5.11.1.1</u> of this standard.

h. Each binding specification SHALL include information about the message protocol that the service uses for this binding, as described in <u>section 5.11.1.2</u> of this standard.

i. Each binding specification SHALL include information about the transport protocol that the service uses for this binding, as described in <u>section 5.11.1.3</u> of this standard.

j. Each binding specification SHALL include information about other protocols that the service uses for this binding, as described in <u>section 5.11.1.4</u> of this standard.

5.11.1.1 Data Protocol

In order to exchange data between <u>SOA</u> components, an agreed-upon <u>format</u> must be used. A data <u>protocol</u> is a formal set of rules governing data encoding and coordination for data exchange among SOA components.

For the purpose of this standard, two categories of data are considered: 1) text-based data (e.g., an <u>XML</u> document) and binary-encoded data (e.g., a <u>PNG</u> image, a Microsoft Excel spreadsheet). The XML format is presently the protocol most often employed for exchanging textual data via <u>Web services</u>. Besides transmitting textual data, an important use for XML is serializing data structures according to domain-specific conceptual models; e.g., the Geography Markup Language (GML) used to serialize information about geographical features or the Aeronautical Information Exchange Model (AIXM) used for transmitting aeronautical information.

Binary-encoded data is data that is converted using a code, frequently consisting of binary numbers or two-dimensional arrays of pixels (a graphical-based encoding). Both XML-based and graphical-based formats are used in today's FAA SOA implementation and, in some scenarios, within the same service implementation; e.g., a Web Map service uses XML to request a map rendered as an <u>SVG</u> image.

a. Section 7.1.1.1 (or 7.1.n.1, as appropriate) of the <u>WSRD</u> SHALL specify the data protocol for this <u>binding</u>.

b. Section 7.1.1.1 (or 7.1.n.1, as appropriate) of the WSRD SHALL specify the <u>normative document</u> that regulates the data protocol.

c. The normative document SHALL be specified as prescribed in <u>section 5.6</u> of this standard.

d. If an accessible reference (e.g., <u>URL</u>) to the normative document is not available, the document itself SHALL be included in an Appendix of the WSRD.

e. The data protocol described in section 7.1.1.1 (or 7.1.n.1, as appropriate) of the WSRD SHALL be compatible with the data defined in section 5.2.4 ("Data Elements") of the WSRD.

f. If there are no data protocol requirements, section 7.1.1.1 (or 7.1.n.1, as appropriate) of the WSRD SHALL include the statement "This WSRD does not impose any data protocol requirements for this binding."

5.11.1.2 Message Protocol

In a <u>SOA</u> environment, the communication and interaction between components is performed by exchanging <u>messages</u> of predefined content. A message <u>protocol</u> is a formal set of rules and conventions governing procedure calls and responses among communicating SOA components.

The most widely used message protocol for Web services is SOAP, a specification that defines an XML-based common message format.

Generally, a message consists of a header part and a message-specific payload. The message header may include directives or contextual information related to the message delivery (e.g. security or addressing information). The message payload consists of instances of service-defined data elements (see section 5.9.2.4 of this standard for requirements for describing payload data).

a. Section 7.1.1.2 (or 7.1.n.2, as appropriate) of the WSRD SHALL specify the message protocol for this binding.

b. The normative document that establishes the message protocol SHALL be specified as prescribed in section 5.6 of this standard.

c. If an accessible reference (e.g., URL) to the normative document is not available, the document itself SHALL be included in an Appendix of the WSRD.

d. The message protocol described in section 7.1.1.2 (or 7.1.n.2, as appropriate) of the WSRD SHALL be compatible with the data protocol specified for this binding and described in section 7.1.1.1 (or 7.1.n.1, as appropriate) of the WSRD.

e. If there are no message protocol requirements, section 7.1.1.2 (or 7.1.n.2, as appropriate) of the WSRD SHALL include the statement "This WSRD does not impose any message protocol requirements for this binding."

5.11.1.3 Transport Protocol

A transport protocol is a formal set of rules governing message transmission and port handling among communicating SOA components.

Various approaches can be used in SOA for transporting messages, and consequently various transport protocols are deployed; e.g., HTTP/HTPPS (traditional approach), JMS (message-based asynchronous approach), and FTP (file-based approach). As explained in section 1.3.2 of this standard, since Web services operate using Internet-based standards, all transport protocols defined in the context of a WSRD use TCP/IP as an underlying protocol.

a. Section 7.1.1.3 (or 7.1.n.3, as appropriate) of the WSRD SHALL specify the transport protocol for this binding.

b. The normative document that establishes the transport protocol SHALL be specified as prescribed in section 5.6 of this standard.

c. If an accessible reference (e.g., URL) to the normative document is not available, the document itself SHALL be included in an Appendix of the WSRD.

d. The transport protocol described in section 7.1.1.3 (or 7.1.n.3, as appropriate) of the WSRD SHALL be compatible with the message protocol specified for this binding and described in section 7.1.1.2 (or 7.1.n.2, as appropriate) of the WSRD.

e. If there are no transport protocol requirements, section 7.1.1.3 (or 7.1.n.3, as appropriate) of the WSRD SHALL include the statement "This WSRD does not impose any transport protocol requirements for this binding."

5.11.1.4 Other Protocols

Some modern protocols may combine data definitions with messaging conventions or messaging and transport governing conventions and cannot be unambiguously classified as strictly a data,

message or transport protocol to be specified in section 7.1.1.1, 7.1.1.2 or 7.1.1.3 of the WSRD. This section of the standard describes requirements for such protocols.

Note: REST (Representational State Transfer), which is becoming popular in SOA-based development, is not a protocol *per se*; rather it is an architectural style that defines a transport and messaging paradigm for developing Web services.

a. Section 7.1.1.4 (or 7.1.n.4, as appropriate) of the WSRD SHALL specify information about other protocols that the service uses for this binding and which cannot be clearly identified as a data protocol, a transport protocol, or a message protocol.

b. The normative document that establishes each described protocol SHALL be specified as prescribed in section 5.6 of this standard.

c. If an accessible reference (e.g., URL) to the normative document is not available, the document itself SHALL be included in an Appendix of the WSRD.

d. If there are no other protocol requirements, section 7.1.1.4 (or 7.1.n.4, as appropriate) of the WSRD SHALL include the statement "This WSRD does not impose any other protocol requirements."

5.11.2 Processing Requirements

Section 7.2 of the WSRD specifies the processing requirements, that is, steps or actions which are required to be taken on data that is received as part of a Web service request (input) in order to produce the desired output (see section 5.9.2.1 for requirements for an operation's input and output). Actions on data might be (but are not limited to) transformations, algorithms, unique logic, or business rules. Examples include special validation that goes beyond checking the XML request as being valid or well-formed (e.g., making sure the ZIP code is valid for the city and state in an address), priority processing requirements, overload handling requirements, or timing limitations (e.g., the maximum time to wait for a data base response).

a. Section 7.2 of the WSRD SHALL specify the processing requirements for the Web service.

b. If there are no processing requirements, section 7.2 of the WSRD SHALL include the statement "This WSRD does not impose any processing requirements."

5.11.3 Operational Environment Requirements

Although Web services are defined as "platform and implementation independent" (see section 1.1), the software components that realize a Web service are usually subject to the constraints of their potential or existing operational environment. A service may be required to be developed in a specific development environment in compliance with the provider organization's established practices, or to run on an existing enterprise network, or to be hosted by a specific set of hardware and/or operating system. Section 7.3 of the WSRD specifies such requirements.

a. Section 7.3 of the WSRD SHALL specify all requirements relative to the environment in which the Web service is developed, operated, and maintained.

b. Section 7.3 of the WSRD SHALL specify software compliance requirements for the Web service.

c. If there are no software compliance requirements, section 7.3 of the WSRD SHALL include the statement "This WSRD does not impose any software compliance requirements."

d. Section 7.3 of the WSRD SHALL specify hardware compliance requirements for the Web service.

e. If there are no hardware compliance requirements, section 7.3 of the WSRD SHALL include the statement "This WSRD does not impose any hardware compliance requirements."

f. Section 7.3 of the WSRD SHALL specify network compliance requirements for the Web service.

g. If there are no network compliance requirements, section 7.3 of the WSRD SHALL include the statement "This WSRD does not impose any network compliance requirements."

h. If compliance for software, hardware, or network is defined in normative documents, the normative documents SHALL be specified as prescribed in section 5.6 of this standard.

i. If an accessible reference (e.g., URL) to a specified normative document is not available, the document itself SHALL be included in an Appendix of the WSRD.

j. Section 7.3 of the WSRD SHALL specify configuration requirements for the Web service for a given operational environment.

k. If there are no configuration requirements, section 7.3 of the WSRD SHALL include the statement "This WSRD does not impose any configuration requirements."

l. Section 7.3 of the WSRD SHALL specify all external databases, data storage devices, and data services that are required to be used by the Web service.

m. Section 7.3 of the WSRD SHALL specify requirements for auditing and monitoring the performance of the Web service.

n. If the capacity of the Web service is an issue, then section 7.3 of the WSRD SHALL specify all hardware and/or software reserve capacity requirements including methods of monitoring the required reserves and alerting operations personnel when the reserves are approached, reached, or exceeded.

o. If it is expected that the Web service will be enhanced after its initial implementation, then section 7.3 of the WSRD SHALL specify all enhanceability requirements identifying the capabilities to add, delete, and adapt software components to provide new and/or improved functionality, capacity, and/or performance relative to their impact on the system architecture.

p. If the usage of the Web service is expected to increase after its initial implementation, then section 7.3 of the WSRD SHALL specify all scalability requirements identifying the capabilities to add, delete, and adapt resources in order to meet the capacity, functionality, and performance required to meet the increased system loads.

5.12 Quality Assurance Provisions

a. Section 8 of the WSRD SHALL specify the process for verification of the requirements contained in the WSRD.

b. The test and evaluation process specified in section 4.12, Verification and Validation, of the System Engineering Manual [14] SHALL be used, and tailored as necessary for the levels and methods of verification identified in the Verification Requirements Traceability Matrix (VRTM).

5.12.1 Responsibility for Verification

a. Section 8.1 of the WSRD SHALL state: "The FAA is responsible for developing and implementing the verification of requirements for each project. The FAA may delegate

verification activities to other organizations, independent contractors, and/or the prime contractor."

5.12.2 Special Verification Requirements

This section describes any special verification requirements necessary to verify the technical requirements imposed within the WSRD.

a. If testing the Web service consumer application requires special arrangements (e.g., establishment of a test database), section 8.2 of the WSRD SHALL state the test requirements and provide the point of contact information to make the arrangements.

b. If testing the Web service consumer application does not require special arrangements, section 8.2 of the WSRD SHALL specify how to report problems with the provider application encountered during testing the consumer application and how they will be resolved.

5.12.3 Verification Requirements Traceability Matrix

There is a one-to-one correspondence between each requirement statement (i.e., the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL") and each entry in the Verification Requirements Traceability Matrix (VRTM). An example of a VRTM is shown in Table III below.

a. Section 8.3 of the WSRD SHALL contain the following statement: "Verification shall be in accordance with Table 8-1, Verification Requirements Traceability Matrix (VRTM)."

b. The content and structure of the VRTM SHALL comply (and be tailored if necessary) with the System Engineering Manual (SEM) [14] section 4.12.

c. The contents of the VRTM SHALL provide verification of each technical requirement contained in the WSRD with the appropriate verification method(s).

d. The verification methods used in the VRTM SHALL be identified at the top of the VRTM.

The appropriate verification levels and methods for use in the VRTM are defined in the following paragraphs.

5.12.3.1 Verification Levels

a. The levels of verification are Service and Integration. All requirements imposed by the WSRD SHALL be verified at one or both of these levels.

  1. Service level (Development). This level is usually conducted at the developer or contractor's facility and culminates in the formal acceptance of a contractual end-item.

  2. Integration level (Quality Assurance). This level is conducted by the service consumer. The verification conducted determines if the consumer application software performs with the service provider application software and service specified in the WSRD in accordance with the operational and functional requirements.

5.12.3.2 Verification Methods

a. The four verification methods that can be used at either of the verification levels are shown in Appendix D, Verification Methods Taxonomy. All requirements imposed by the WSRD SHALL be verified using one or more of the values selected from this taxonomy.

TABLE III. Sample verification requirements traceability matrix

A = Analysis; D = Demonstration; I = Inspection; T = Test; X = Not Applicable

Section Number	Requirement Title	Requirement ID	Verification Level	
			Service Level	Integration Level
5.1	Service Business Functions			
		1	D	D
		2	A	A
		3	I	I
		n	D	D
5.2	Service Interfaces			
		1	D	D
		2	D	D
		3	I, D	D
		n	I	X

6 APPENDIXES

6.1 Appendix A. Example of a WSRD Cover Page

U.S. Department of
Transportation
**Federal Aviation
Administration**

**Web Service Requirements Document
Special Activity Airspace Management Web Service,
Aeronautical Information Management (AIM)**

6.2 Appendix B. Example of a WSRD Approval Signature Page

**Web Service Requirements Document
Special Activity Airspace Management Web Service,
Aeronautical Information Management (AIM)**

Approval Signatures

Name	Organi-zation	Signature	Date Signed

i

6.3 Appendix C. Example of a WSRD Revision Record Page

FAA-X-XXX
Revision A
September 4, 2012

Revision Record

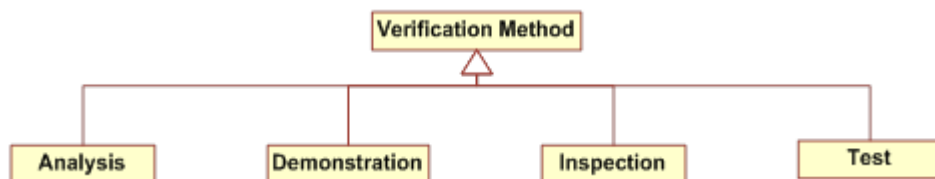| Revision Letter	Description	Revision Date	Entered By

ii

46

6.4 Appendix D. Verification Method Taxonomy

title	Verification Method
namespace	urn:us:gov:dot:faa:taxonomies:verification-method
description	The Verification Method taxonomy is used to categorize the methods for verifying requirements.
creator	Terminal Engineering, AJT-131
source	FAA-STD-025f, Preparation of Interface Documentation
rights	The taxonomy is in the public domain and may therefore be reproduced without any limitations.

The purpose of this taxonomy is to provide a single standard system for classifying FAA verification methods that are used in various requirements documents.

The taxonomy is maintained as a registered artifact in the FAA Data Registry (FDR) tool in accordance with FAA Order 1375.1 [3] and is available at the FDR Web site, http://fdr.gov/fdr/Home.jsp.

Structure

List of Values

ID	Parent ID	Name	Allowed	Description
verification-method		Verification Method	No	One or more of the methods used to verify a given requirement.
analysis	verification-method	Analysis	Yes	A method in which hardware or software designs are compared with known scientific and technical principles, procedures, and practices to estimate the capability of the proposed design to meet the mission and system requirements.
demonstration	verification-method	Demonstration	Yes	A method in which qualitative determination of properties is made for a configuration item, including software and/or the use of technical data and documentation. The items being verified are observed, but not quantitatively measured, in a dynamic state.

ID	Parent ID	Name	Allowed	Description
inspection	verification-method	Inspection	Yes	A method used to determine compliance without using special laboratory equipment, procedures, or services and consists of a nondestructive static-state examination of hardware, software, and/or technical data and documentation.
test	verification-method	Test	Yes	A method in which performance is measured during or after the controlled application of functional and/or environmental stimuli. Quantitative measurements are analyzed to determine the degree of compliance. The process uses standardized laboratory equipment, procedures, and/or services.