

Using Web Services for Business – Glossary

■ This glossary explains many of the terms and ideas in David Burdett's article on "Using Web Services for Business" Some are specific to Web services. Others have more general applicability. However, in this paper, their use of the term as they apply to Web services is the main way in which they are described.

The descriptions also identify many links to further information on the Web.

Address Route: An Address Route describes the set of Web addresses through which a Web Service message (i.e. a SOAP Message) is sent from when it is first created until it reaches its final destinations.

Address Routing: See *Address Route*

Agreements: An Agreement describes how two, sometimes more, businesses have agreed to carry out business with each other electronically. They are typically created by comparing one business' use of profiles and policies with the other business' use and selecting and agreeing a subset of technology that both support. They are identified with an Agreement Identifier.

Agreement Identifier: An Agreement Identifier is a unique identifier that identifies an agreement. Agreement Identifiers are often carried in the SOAP Headers of a SOAPMessage so that the agreement that applies to the processing of a message can be determined by the recipient of the message

Attachment: Attachments are additional documents sent at the same and in the same message as a main business document. Attachments can be both XML and non-XML. To include an attachment, methods such as MIME, DIME or SOAP with Attachments have to be used to combine all the parts together into one message.

Authentication: Authentication is the process by which a recipient of a message, such as a SOAP Message, can determine the identity of the sender of the message with

certainty. This often involves the sender of a message digitally signing the message using a digital certificate and the recipient of the message checking the digital signature for accuracy when the message is received.

Authorization: Authorization is the process of checking that a request implied by the receipt of a message, e.g. a SOAP Message is one that the sender of the message is allowed to make and therefore the request should be acted on by the service that receives it.

Basic Profile: The WS-I Basic Profile is one of the activities of WS-I. It is a specification that provides precise rules on how the basic Web Services specifications of SOAP 1.1, WSDL 1.1 and UDDI 2.0 should be used together in order to maximize interoperability

Business Document: A Business Document is a name for the documents such as orders, invoices, shipment notices or any other document that is exchanged between businesses in order to carry out business

Business Transaction: A Business Transaction is an instance of two or more businesses carrying out business. For example a buyer placing an order with a seller.

Business Transaction Protocol: The Business Transaction Protocol of BTP is a protocol that allows the synchronization of data between remote servers using an XML based protocol using the ideas of two-phase commit. BTP is a Technical Committee within OASIS see [www.oasis-](http://www.oasis-
open.org/committees/tchome.php?wg_abbrev=business-transaction)

[open.org/committees/tchome.php?wg_abbrev=business-transaction](http://www.oasis-open.org/committees/tchome.php?wg_abbrev=business-transaction)

Callback Address: See return address

Conversation: A conversation is a set of related messages. For example the set of messages used by a buyer to place an order, the seller to provide a response, and the buyer to make multiple changes through sending change orders. Conversation instances are identified with a Conversation Identifier

Conversation Identifier: A

Conversation Identifier is a unique identifier for an instance of a choreography. For example, the exchange of messages required to complete the placement of an order could have a choreography identifier associated with them. Choreography identifiers are transported in SOAP Headers of a SOAP Message so that the conversation being executed can be identified.

Delivery Receipt: A Delivery Receipt is a message, usually a SOAP Message that is returned by a recipient of an earlier message to indicate to the sender of the earlier message that the message was received.

Digital Signature: A Digital Signature is a way of signing an electronic document in a similar way to a pen can be used by a person to sign a paper document. This means that a digital signature can be used to determine the authenticity of a business document or message. Digital signatures can also be used to ensure that any alterations to a business document can always be detected. See also XML Signature. Digital signatures are created and checked using a Digital Certificate.

Digital Certificate: A Digital Certificate is a set of codes that are used to create and verify a digital signature and/or encrypt a message or XML document. Digital Certificates can be thought of as "keys" that can be used to lock or unlock a document. See also key management.

DIME: Direct Internet Message Encapsulation (DIME) was a specification for combining multiple documents into a single SOAP Message. It was originally developed by IBM and Microsoft and was submitted to the IETF as an Internet Draft.

The DIME specification however has not been progressed and the Internet Draft published at the IETF has been allowed to lapse see www.ietf.org/internet-drafts/draft-nielsen-dime-03.txt. The original specification is available at

<http://msdn.microsoft.com/library/en-us/dnglobspec/html/draft-nielsen-dime-02.txt>

See also *SOAP with Attachments*.

Direct Internet Message

Encapsulation: See *DIME*

Document: In a Web services context, a document is the data that is placed in the content or payload of a SOAP Message. A document can be placed either in the SOAP Body or in an attachment. Documents are often business documents

Document Definitions: A Document Definition, is a definition of a document in a definition language. Document definitions are usually written using XML or XML Schema.

Encryption: Encryption is a method by which data can be scrambled so that it cannot be understood by anyone unless they have the key to unscramble it. XML or other data can be encrypted using the XML Encryption standard.

Intellectual Property: Intellectual property is associated with unique and novel ideas over which a business claims rights. Patents and copyrights are used to establish those rights. Once a business has established those rights, they can then require other businesses to get a license from them before using those ideas. Granting of a license can often involve the payment of fees.

Patents and copyright have been established around many of the software ideas associated with Web Services.

IP: See *intellectual property*

Key Management: Key Management is the management of the processes required for creating, updating, distributing and deprecating the keys or digital certificates required to generate digital signatures or to encrypt documents. The XML Key Management Working Group in the W3C is addressing the distribution part of Key Management with the XKMS specification. See www.w3.org/2001/XKMS

Liberty Alliance: The Liberty Alliance is standards group that is developing a set of specifications for federated identity services. It allows users to link identity information between accounts without centrally storing personal information. See www.projectliberty.org/

Logical Address: A logical address is an identifier or an address for a Web Service that identifies who is running the service

and what it does rather than where it is located on the Web. For example urn:www-dnb-com/dunsno/123456789012345/sale-order could identify the sales order service operated by the company with the DUNS no 1234567890 12345. Logical addresses usually need to be mapped to a physical address before a SOAP Message can be sent. Logical addresses usually remain the same even when the physical address has changed.

Message: A message consists of an envelope and its contents. For Web Services it is a SOAP Envelope with a business document contained in the SOAP Body. Messages are created by one service and then sent to another service that processes them. A Message can also contain additional documents as an attachment.

Message Correlation: Message correlation is the idea of relating one message that is sent with its reply. Typically, the first message contains a Message Identifier in a SOAP Header that is then included in the SOAP Header of any reply

Message Encryption: Message encryption is the process of scrambling a message so that its contents are not decipherable by anyone who does not have access to the digital certificate required to unscramble the message. See also encryption.

Message Envelope: A message envelope is a way of electronically grouping together the different message parts within a message. For Web services, a message envelope is always a SOAP envelope

Message Expiry: Message expiry is information typically stored in the SOAP Header of a message that indicates to the recipient of the message the time after which the message should no longer be processed

Message Identifier: A message identifier is a unique identifier for a message that allows the message to be referenced and retrieved. They are often Globally Unique Identifiers or GUIDs which means that no two identifiers are ever the same. Message Identifiers are stored in the SOAP Header of a message. See also Message Correlation.

Message Part: A message part contains a discrete separate part of a message. Message parts can be located in the SOAP Body or in an attachment

Message Privacy: Message privacy is the idea of protecting the contents of a

message from viewing by people or software that are not authorized to see it. Encryption techniques are usually used to do this. See also Message Encryption and SSL.

Message Routing: Message routing is the process of specifying the servers through which a message passes when it is sent from the original creator of the message to its final destination.

Message Security: Message security involves one or more of: making sure that a message has not been tampered through the use of a digital signature, is kept private using Message Privacy, is authentic and authorized. See also *Message Privacy* and *Message Encryption*.

Message Sequencing: Message sequencing is the idea of making sure that messages are processed in the same sequence at the destination as the sequence in which they were sent even if some of the messages were delayed so that some messages arrive after messages that were sent later

OASIS: Organization for the Advancement of Structured Information Standards. A not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards. Together with the W3C, it is the home for the development of many of the standards used by Web Services. See www.oasis-open.org

Physical Address: A physical address is the location of a service on the Web. It is typically defined as a URL. See also Logical Address

Privacy: Privacy is the process of making sure that only those that are allowed can see a message or its contents. The techniques used involve encryption. See also XML Encryption and SSL.

Reliable Messaging: Reliable Messaging is a protocol that allows a message to be delivered to its destination with a high probability that the message will be delivered. Reliable messaging works by requesting an acknowledgement message be sent in return to a message that was sent. If no acknowledgement is received after a period of time, the original message is resent until the acknowledgement arrives or the original sender gives up.

Return Address: A return address is information stored in a SOAP Header that indicates to the recipient of the message where a reply to the message should be

sent. It is also sometimes known as a callback address.

Secure Sockets Layer: See *SSL*

SMTOM: See SOAP Message Transmission Optimization Mechanism
SMTP Simple Mail Transport Protocol (SMTP) is a widely used protocol for sending e-mail messages. All e-mail systems that use the Internet use SMTP for sending messages between one email server and another. SMTP is built on top of TCP/IP. See www.ietf.org/rfc/rfc1123.txt

SOAP Body: The SOAP Body is the second part of the SOAP Envelope. It contains the payload of the message typically in the form of a business document

SOAP Envelope: The SOAP Envelope is the outermost part of a SOAP Message. It contains a SOAP Header and a SOAP Body

SOAP Header: The SOAP Header is the first part of the SOAP envelope and contains additional information about the message such as Address Routing, Conversation Identifiers, Digital Signatures, Message Correlation, Message Expiry, and Message Identifiers.

SOAP Message: A SOAP Message is a SOAP Envelope wrapped in a transport protocol such as HTTP or SMTP.

SOAP Message Transmission Optimization Mechanism: The SOAP Message Transmission Optimization Mechanism (SMTOM) provides "a concrete implementation of it for optimizing the transmission and/or wire format of SOAP messages." This provides a mechanism for transporting multiple different parts of a message while still allowing the message to appear as XML to the application that is processing it. It is based on the ideas of PASWA See www.w3.org/TR/soap12-mtom/

SOAP with Attachments: SOAP with Attachments is a specification that describes how to carry a SOAP Envelope with attachments using MIME. See www.w3.org/TR/SOAP-attachments

SOAP Simple Object Access Protocol (SOAP) is a protocol that describes how two servers can interact with each other by exchanging information in SOAP messages. A SOAP Message consists of SOAP Envelope with a SOAP Header and a SOAP Body. The original version of SOAP is version 1.1, this being replaced by version 1.2.

SOAP 1.1: The original version of SOAP. See www.w3.org/TR/SOAP/

SOAP 1.2: The replacement for SOAP

version 1.1. SOAP Version 1.2 is being developed in the W3C see www.w3.org/TR/soap12-part1.

SSL: Secure Sockets Layer (SSL) is a protocol for sending or transmitting private messages via the Internet. It works by encrypting any data that is sent over a connection. By convention, URLs that start with https: instead of http: are using SSL. See also XML Encryption.

Transport Security: Transport security is a method of encrypting a message as it is sent between servers. See *SSL*

Two-Phase Commit: Two-phase commit is a process by which two processes running at separate locations can synchronize what they do so that, at both ends, everything works or nothing works. It is based on the ideas of two-phase commit used with distributed databases to make sure that multiple copies of a database are always identical

UDDI: Universal Description, Discovery and Implementation (UDDI) is a standard for storing, searching, and managing information in registries. It is a technical committee within OASIS. See www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec

UDDI 2.0: UDDI 2.0 is the version of UDDI that is used to create the Basic Profile within WS-I.

Universal Discovery Description and Integration: See *UDDI*

W3C: The World Wide Web Consortium is the original standards setting authority that developed many of the original standards for the Web such as HTML and HTTP. Together with OASIS, it is the home for development of many of the standards used by Web services. See www.w3.org

Web Services Interoperability Organization: See *WS-I*

Web Services Middleware: Web services middleware is software that supports Web services standards, protocols, and principles providing a convenient set of APIs that an application programmer can use to develop Web services.

Web Services Transaction Management: The Web Services Transaction Management (WS-TXM) specification developed by Arjuna, Fujitsu, IONA, Oracle, and Sun provides a mechanism for handling the problems that can occur when multiple different business transactions need to cooperate and one of them fails causing the other

business transactions to take some compensatory action. See www.arjuna.com/library/specs/wscaf_1-0/WS-TXM.pdf

World Wide Web Consortium: See *W3C*

WS Acknowledgement: *WS Acknowledgement* is a specification published by BEA that "allows a sender of a message to request that an acknowledgement is sent in a response." See http://dev2dev.bea.com/technologies/webservices/WS-Acknowledgement-0_9.jsp

WS Addressing: *WS Addressing* is a specification published by IBM, BEA, and Microsoft that "provides transport-neutral mechanisms to address Web services and messages." See <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-addressing.asp>

WS Authorization: *WS Authorization* is a specification that IBM and Microsoft plan to develop that will "describe how to manage authorization data and authorization policies".

WS Callback: *WS Callback* is a specification published by BEA in February 2003 that is "used to dynamically specify where to send asynchronous responses to a SOAP request." See http://dev2dev.bea.com/technologies/webservices/WS-Callback-0_9.jsp

WS-Context: The *WS-Context* specification published by Sun, Oracle, Iona, Arjuna, and Fujitsu provides a mechanism for sharing context information between a set of Web services that are taking part in some common process. See www.arjuna.com/library/specs/ws_caf_1-0/WS-CTX.pdf

WS-Coordination: *WS-Coordination* is a specification developed by IBM, Microsoft, and BEA. It "describes an extensible framework for providing protocols that coordinate the actions of distributed applications." See www-106.ibm.com/developerworks/library/ws-coor

WS-I: The *Web Services Interoperability Organization* is an "open, industry organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages." See www.ws-i.org

WS-MessageData: *WS-MessageData* is a specification published by BEA. It provides metadata definitions for Message Identity.

See http://dev2dev.bea.com/technologies/webservices/WS-MessageData-0_9.jsp

WS Policy: WS Policy is a specification developed by IBM, Microsoft, BEA, and SAP that provides “a general-purpose model and corresponding syntax to describe and communicate the policies of a Web service.” See <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-policy.asp>

WS-PolicyAssertions: The Web Services Policy Assertions Language is a specification published by IBM, Microsoft, and SAP. The specification “defines general messaging-related assertions for use with WS-Policy.” See <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-policyassertions.asp>

WS PolicyAttachments: The Web Services Policy Attachment is a specification published by IBM, Microsoft, BEA and SAP. It “specifies three specific attachment mechanisms for using policy expressions with existing XML Web service technologies.” See www-106.ibm.com/developerworks/library/ws-polatt/

WS-Reliability: WS-Reliability is a specification published by Sonic, Sun, NEC, Fujitsu, Oracle, and Hitachi that defines a protocol “for exchanging SOAP messages with guaranteed delivery, no duplicate s, and guaranteed message ordering.” See <http://sunonedev.sun.com/platform/technologies/ws-reliability.v1.0.pdf>

WS-ReliableMessaging: The WS-Reliable Messaging Protocol is a specification published by BEA, Microsoft, Tibco, and IBM. It “describes a protocol that allows messages to be delivered reliably between distributed applications in the presence of software component, system, or network failures.” See <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-reliablemessaging.asp>

WS-Routing: WS-Routing is a specification published by Microsoft that “defines mechanisms for routing SOAP messages.” See <http://msdn.microsoft.com/library/default.aspx?url=/library/en-us/dnglobspec/html/wsrouspecindex.asp>

WS-SecureConversation: The WS-Secure Conversation Language is a specification developed by IBM, Microsoft, Verisign, and RSA Security that “defines extensions that build on WS Security to provide secure communication. Specifically, it defines mechanisms for establishing and sharing security

contexts, and deriving session keys from security contexts.” See <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-secureconversation.asp>

WS-Security: The WS-Security specification developed by IBM, Microsoft, and RSA describes “enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication.” See www-106.ibm.com/developerworks/webservices/library/ws-secure/

WS-Transaction: The WS-Transaction is a specification developed by IBM, BEA and Microsoft was published. It “describes coordination types that are used with the extensible coordination framework described in the WS-Coordination specification.” See www-106.ibm.com/developerworks/library/ws-transpec/

WS-Trust: The WS-Trust Language is a specification developed by IBM, Microsoft, Verisign, and RSA Security that “defines extensions that build on WS Security to request and issue security tokens and to manage trust relationships.” See <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-trust.asp>

WSDL: The Web Services Description Language is a specification developed by IBM and Microsoft that defines “an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.” Version 1.2 of WSDL is being developed in the W3C. See www.w3.org/2002/ws/desc

WSDL 1.1: The first version of the WSDL Specification. See www.w3.org/TR/wsdl

XML Encryption: XML Encryption is an activity within the W3C that has developed a specification for “a process for encrypting data and representing the result in XML.” See www.w3.org/TR/xmlenc-core

XML Signature: XML Signature is the activity within the W3C that specified a way of digitally signing a document using XML. See www.w3.org/Signature ©