Web Services Atomic Transaction (WS-AtomicTransaction) 1.1

Committee Draft 01, March 15, 2006

Document Identifier:

wstx-wsat-1.1-spec-cd-01

Location:

http://docs.oasis-open.org/ws-tx/wstx-wsat-1.1-spec-cd-01.pdf

Technical Committee:

OASIS WS-TX TC

Chair(s):

Eric Newcomer, Iona
Ian Robinson, IBM

Editor(s):

Mark Little, JBoss Inc. <mark.little@jboss.com>
Andrew Wilkinson, IBM <awilkinson@uk.ibm.com>

Abstract:

This specification provides the definition of the atomic transaction coordination type that is to be used with the extensible coordination framework described in the WS-Coordination specification. The specification defines three specific agreement coordination protocols for the atomic transaction coordination type: completion, volatile two-phase commit, and durable two-phase commit. Developers can use any or all of these protocols when building applications that require consistent agreement on the outcome of short-lived distributed activities that have the all-or-nothing property.

Status:

This document is published by the WS-TX TC as a “committee draft".

This document was last revised or approved by the WS-TX TC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at www.oasis-open.org/committees/ws-tx .

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (www.oasis-open.org/committees/ws-tx/ipr.php).

The non-normative errata page for this specification is located at www.oasis-open.org/committees/ws-tx .

Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification, can be obtained from the OASIS President.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS President.

Table of contents

1 Note on terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [KEYWORDS].

Namespace URIs of the general form http://example.org and http://example.com represents some application-dependent or context-dependent URI as defined in RFC 2396 [URI].

1.1 Composable Architecture

By using the SOAP [SOAP]and WSDL [WSDL] extensibility model, SOAP-based and WSDL-based specifications are designed to work together to define a rich Web services environment. As such, WS-AtomicTransaction by itself does not define all features required for a complete solution. WS-AtomicTransaction is a building block used with other specifications of Web services (e.g., WS-Coordination, WS-Security) and application-specific protocols that are able to accommodate a wide variety of coordination protocols related to the coordination actions of distributed applications.

1.2 Namespace

The XML namespace URI that MUST be used by implementations of this specification is:

```
http://docs.oasis-open.org/ws-tx/wsat/2006/03
```

This is also used as the CoordinationContext type for atomic transactions.

1.2.1 Prefix Namespace

Prefix	Namespace
S	http://www.w3.org/2003/05/soap-envelope
wscoor	http://docs.oasis-open.org/ws-tx/wscoor/2006/03
wsat	http://docs.oasis-open.org/ws-tx/wsat/2006/03

If an action URI is used then the action URI MUST consist of the wsat namespace URI concatenated with the "/" character and the element name. For example:

```
http://docs.oasis-open.org/ws-tx/wsat/2006/03/Commit
```

1.3 XSD and WSDL Files

The following links hold the XML schema and the WSDL declarations defined in this document.

http://docs.oasis-open.org/ws-tx/wsat/2006/03/wsat.xsd

http://docs.oasis-open.org/ws-tx/wsat/2006/03/wsat.wsdl

Soap bindings for the WSDL documents defined in this specification MUST use "document" for the *style* attribute.

1.4 AT Protocol Elements

The protocol elements define various extensibility points that allow other child or attribute content. Additional children and/or attributes MAY be added at the indicated extension points but MUST NOT contradict the semantics of the parent and/or owner, respectively. If a receiver does not recognize an extension, the receiver SHOULD ignore the extension.

1.5 Normative References

1.6 Non-normative References

[KEYWORDS]

S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997

[SOAP]

W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000

[URI]

T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396, MIT/LCS, U.C. Irvine, Xerox Corporation, August 1998

[XML-ns]

W3C Recommendation, "Namespaces in XML," 14 January 1999

[XML-Schema1]

W3C Recommendation, "XML Schema Part 1: Structures," 2 May 2001

[XML-Schema2]

W3C Recommendation, "XML Schema Part 2: Datatypes," 2 May 2001

[WSCOOR]

Web Services Coordination (WS-Coordination) 1.1, OASIS, March 2006

[WSADDR]

Web Services Addressing (WS-Addressing), Microsoft, IBM, Sun, BEA Systems, SAP, Sun, August 2004

[WSPOLICY]

Web Services Policy Framework (WS-Policy), VeriSign, Microsoft, Sonic Software, IBM, BEA Systems, SAP, September 2004

[WSPOLICYATTACH]

Web Services Policy Attachment (WS-PolicyAttachment), VeriSign, Microsoft, Sonic Software, IBM, BEA Systems, SAP, September 2004

[WSDL]

Web Services Description Language (WSDL) 1.1

"http://www.w3.org/TR/2001/NOTE-wsdl-20010315"

[WSSec]

OASIS Standard 200401, March 2004, "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)"

[WSSecPolicy]

Web Services Security Policy Language (WS-SecurityPolicy), Microsoft, VeriSign, IBM, RSA Security, July 2005

[WSSecConv]

Web Services Secure Conversation Language (WS-SecureConversation), OpenNetwork, Layer7, Netegrity, Microsoft, Reactivity, IBM, VeriSign, BEA Systems, Oblix, RSA Security, Ping Identity, Westbridge, Computer Associates, February 2005

[WSTrust]

Web Services Trust Language (WS-Trust), OpenNetwork, Layer7, Netegrity, Microsoft, Reactivity, VeriSign, IBM, BEA Systems, Oblix, RSA Security, Ping Identity, Westbridge, Computer Associates, February 2005.

2 Introduction

The current set of Web service specifications [WSDL] [SOAP] defines protocols for Web service interoperability. Web services increasingly tie together a number of participants forming large distributed applications. The resulting activities may have complex structure and relationships.

The WS-Coordination specification defines an extensible framework for defining coordination types. This specification provides the definition of an atomic transaction coordination type used to coordinate activities having an "all or nothing" property. Atomic transactions commonly require a high level of trust between participants and are short in duration. The Atomic Transaction specification defines protocols that enable existing transaction processing systems to wrap their proprietary protocols and interoperate across different hardware and software vendors.

To understand the protocol described in this specification, the following assumptions are made:

- The reader is familiar with existing standards for two-phase commit protocols and with commercially available implementations of such protocols. Therefore this section includes only those details that are essential to understanding the protocols described.
- The reader is familiar with the WS-Coordination [WSCOOR] specification that defines the framework for the WS-AtomicTransaction coordination protocols.
- The reader is familiar with WS-Addressing [WSADDR] and WS-Policy [WSPOLICY].

Atomic transactions have an all-or-nothing property. The actions taken prior to commit are only tentative (i.e., not persistent and not visible to other activities). When an application finishes, it requests the coordinator to determine the outcome for the transaction. The coordinator determines if there were any processing failures by asking the participants to vote. If the participants all vote that they were able to execute successfully, the coordinator commits all actions taken. If a participant votes that it needs to abort or a participant does not respond at all, the coordinator aborts all actions taken. Commit makes the tentative actions visible to other transactions. Abort makes the tentative actions appear as if the actions never happened. Atomic transactions have proven to be extremely valuable for many applications. They provide consistent failure and recovery semantics, so the applications no longer need to deal with the mechanics of determining a mutually agreed outcome decision or to figure out how to recover from a large number of possible inconsistent states.

Atomic Transaction defines protocols that govern the outcome of atomic transactions. It is expected that existing transaction processing systems wrap their proprietary mechanisms and interoperate across different vendor implementations.

3 Atomic Transaction Context

Atomic Transaction builds on WS-Coordination, which defines an activation and a registration service. Example message flows and a complete description of creating and registering for coordinated activities is found in the WS-Coordination specification [WSCOOR].

The Atomic Transaction coordination context must flow on all application messages involved with the transaction.

Atomic Transaction adds the following semantics to the CreateCoordinationContext operation on the activation service.

- If the request includes the CurrentContext element, the target coordinator is interposed as a subordinate to the coordinator stipulated inside the CurrentContext element.
- If the request does not include a CurrentContext element, the target coordinator creates a new transaction and acts as the root.

A coordination context may have an Expires attribute. This attribute specifies the earliest point in time at which a transaction may be terminated solely due to its length of operation. From that point forward, the transaction manager may elect to unilaterally roll back the transaction, so long as it has not transmitted a Commit or a Prepared notification.

The Atomic Transaction protocol is identified by the following coordination type:

```
http://docs.oasis-open.org/ws-tx/wsat/2006/03
```

4 Atomic Transaction Protocols

This specification defines the following protocols for atomic transactions.

- **Completion:** The completion protocol initiates commitment processing. Based on each protocol's registered participants, the coordinator begins with Volatile 2PC then proceeds through Durable 2PC. The final result is signaled to the initiator.
- **Two-Phase Commit (2PC)**: The 2PC protocol coordinates registered participants to reach a commit or abort decision, and ensures that all participants are informed of the final result. The 2PC protocol has two variants:
    - **Volatile 2PC:** Participants managing volatile resources such as a cache should register for this protocol.
    - **Durable 2PC:** Participants managing durable resources such as a database should register for this protocol.

A participant can register for more than one of these protocols by sending multiple Register messages.

4.1 Preconditions

The correct operation of the protocols requires that a number of preconditions MUST be established prior to the processing:

1. The source MUST have knowledge of the destination's policies, if any, and the source MUST be capable of formulating messages that adhere to this policy.
2. If a secure exchange of messages is required, then the source and destination MUST have a security context.

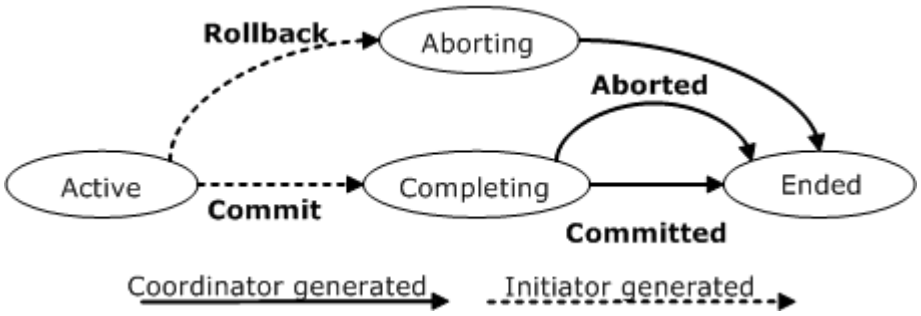
4.2 Completion Protocol

The Completion protocol is used by an application to tell the coordinator to either try to commit or abort an atomic transaction. After the transaction has completed, a status is returned to the application.

An initiator registers for this protocol using the following protocol identifier:

```
http://docs.oasis-open.org/ws-tx/wsat/2006/03/Completion
```

The diagram below illustrates the protocol abstractly:



154
155
156 The coordinator accepts:

157 Commit

158 Upon receipt of this notification, the coordinator knows that the participant has completed
159 application processing and that it should attempt to commit the transaction.

160 Rollback

161 Upon receipt of this notification, the coordinator knows that the participant has terminated
162 application processing and that it should abort the transaction.

163 The initiator accepts:

164 Committed

165 Upon receipt of this notification, the initiator knows that the coordinator reached a decision to
166 commit.

167 Aborted

168 Upon receipt of this notification, the initiator knows that the coordinator reached a decision to
169 abort.

170 Conforming implementations must implement Completion.

171 4.3 Two-Phase Commit Protocol

172 The Two-Phase Commit (2PC) protocol is a Coordination protocol that defines how multiple participants
173 reach agreement on the outcome of an atomic transaction. The 2PC protocol has two variants: Durable
174 2PC and Volatile 2PC.

175 4.3.1 Volatile Two-Phase Commit Protocol

176 Upon receiving a Commit notification in the completion protocol, the root coordinator begins the prepare
177 phase of all participants registered for the Volatile 2PC protocol. All participants registered for this
178 protocol must respond before a Prepare is issued to a participant registered for Durable 2PC. Further
179 participants may register with the coordinator until the coordinator issues a Prepare to any durable
180 participant. A volatile recipient is not guaranteed to receive a notification of the transaction's outcome.

181 Participants register for this protocol using the following protocol identifier:

182 `http://docs.oasis-open.org/ws-tx/wsat/2006/03/Volatile2PC`

4.3.2 Durable Two-Phase Commit Protocol

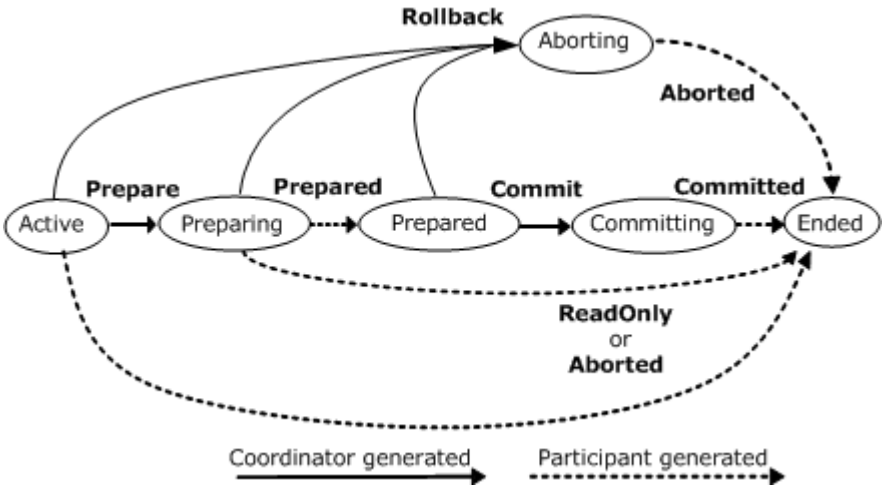
After receiving a Commit notification in the completion protocol and upon successfully completing the prepare phase for Volatile 2PC participants, the root coordinator begins the Prepare phase for Durable 2PC participants. All participants registered for this protocol must respond Prepared or ReadOnly before a Commit notification is issued to a participant registered for either protocol.

Participants register for this protocol using the following protocol identifier:

```
http://docs.oasis-open.org/ws-tx/wsat/2006/03/Durable2PC
```

4.3.3 2PC Diagram and Notifications

The diagram below illustrates the protocol abstractly:



The participant accepts:

Prepare

Upon receipt of this notification, the participant knows to enter phase 1 and vote on the outcome of the transaction. If the participant does not know of the transaction, it must vote to abort. If the participant has already voted, it should resend the same vote.

Rollback

Upon receipt of this notification, the participant knows to abort, and forget, the transaction. This notification can be sent in either phase 1 or phase 2. Once sent, the coordinator may forget all knowledge of this transaction.

Commit

Upon receipt of this notification, the participant knows to commit the transaction. This notification can only be sent after phase 1 and if the participant voted to commit. If the participant does not know of the transaction, it must send a Committed notification to the coordinator.

The coordinator accepts:

Prepared

Upon receipt of this notification, the coordinator knows the participant is prepared and votes to commit the transaction.

ReadOnly

Upon receipt of this notification, the coordinator knows the participant votes to commit the transaction, and has forgotten the transaction. The participant does not wish to participate in phase 2.

Aborted

Upon receipt of this notification, the coordinator knows the participant has aborted, and forgotten, the transaction.

Committed

Upon receipt of this notification, the coordinator knows the participant has committed the transaction. That participant may be safely forgotten.

Replay

Upon receipt of this notification, the coordinator may assume the participant has suffered a recoverable failure. It should resend the last appropriate protocol notification.

Conforming implementations MUST implement the 2PC protocol.

5 AT Policy Assertion

WS-Policy Framework [WS-Policy] and WS-Policy Attachment [WS-PolicyAttachment] collectively define a framework, model and grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web services-based system. To enable a web service to describe transactional capabilities and requirements of a service and its operations, this specification defines a pair of Atomic Transaction policy assertions that leverage the WS-Policy framework.

5.1 Assertion Model

The AT policy assertions are provided by a web service to qualify the transactional processing of messages associated with the particular operation to which the assertions are scoped. The AT policy assertions indicate:

1. whether a requester MAY, MUST or SHOULD NOT include an AtomicTransaction CoordinationContext flowed with the message.
2. the capability of the target service to process the message under an atomic transaction regardless of whether the requester supplies an AtomicTransaction CoordinationContext.

The AT policy assertions are semantically independent of one another, and may be used together or in isolation.

5.2 Normative Outline

The normative outlines for the AT policy assertions are:

```
<wsat:ATAssertion [wsp:Optional="true"]? ... >
  ...
</wsat:ATAssertion>
```

The following describes additional, normative constraints on the outline listed above:

/wsat:ATAssertion

A policy assertion that specifies that an atomic transaction MUST be flowed inside a requester's message. From the perspective of the requester, the target service that processes the transaction MUST behave as if it had participated in the transaction. The transaction MUST be represented as a SOAP header in CoordinationContext format, as defined in WS-Coordination [WS-Coordination].

/wsat:ATAssertion/@wsp:Optional="true"

Per WS-Policy [WS-Policy], this is compact notation for two policy alternatives, one with and one without the assertion. Presence of both policy alternatives indicates that the behavior indicated by the assertion is optional, such that an atomic transaction MAY be flowed inside a requester's message. The absence of the assertion is interpreted to mean that a transaction SHOULD NOT be flowed inside a requester's message.

```
<wsat:ATAlwaysCapability ... />
```

The following describes additional, normative constraints on the outline listed above:

/wsat:ATAlwaysCapability

A policy assertion that specifies a capability of the target service indicating that a requester's message will be processed transactionally regardless of whether the requester supplies an AtomicTransaction CoordinationContext. If an AtomicTransaction context is provided by the requester, it will be used. Otherwise the processing of the message will be within a transaction implicitly started and ended by the target service's environment as part of the processing of that message.

5.3 Assertion Attachment

Because the AT policy assertions indicate atomic transaction behavior for a single operation, the assertions have Operation Policy Subject [WS-PolicyAttachment].

WS-PolicyAttachment defines two WSDL [WSDL 1.1] policy attachment points with Operation Policy Subject:

- wsdl:portType/wsdl:operation – A policy expression containing the AT policy assertion MUST NOT be attached to a wsdl:portType; the AT policy assertions specify a concrete behavior whereas the wsdl:portType is an abstract construct.
- wsdl:binding/wsdl:operation – A policy expression containing the AT policy assertions SHOULD be attached to a wsdl:binding.

5.4 Assertion Example

An example use of the AT policy assertion follows:

```
(01)  <wsdl:definitions
(02)      targetNamespace="bank.example.com"
(03)      xmlns:tns="bank.example.com"
(04)      xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
(05)      xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
(06)      xmlns:wsat="http://docs.oasis-open.org/ws-tx/wsat/2006/03"
(07)      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" >
(08)
(09)    <wsp:Policy wsu:Id="TransactedPolicy1" >
(10)      <wsat:ATAssertion wsp:optional="true" />
(11)      <!-- omitted assertions -->
(12)    </wsp:Policy>
(13)    <wsp:Policy wsu:Id="TransactedPolicy2" >
(14)      <wsat:ATAlwaysCapability />
(15)      <!-- omitted assertions -->
(16)    </wsp:Policy>
(17)    <!-- omitted elements -->
(18)    <wsdl:binding name="BankBinding" type="tns:BankPortType" >
(19)      <!-- omitted elements -->
```

```
(20)      <wsdl:operation name="QueryBalance" >
(21)        <wsp:PolicyReference URI="#TransactedPolicy2"
wsdl:required="true" />
(22)        <!-- omitted elements -->
(23)      </wsdl:operation>
(24)      <wsdl:operation name="TransferFunds" >
(25)        <wsp:PolicyReference URI="#TransactedPolicy1"
wsdl:required="true" />
(26)        <!-- omitted elements -->
(27)      </wsdl:operation>
(28)    </wsdl:binding>
(29)  </wsdl:definitions>
```

Lines (9-12) are a policy expression that includes an AT policy assertion (Line 10) to indicate that an atomic transaction in WS-Coordination [WS-Coordination] format MAY be used.

Lines (13-16) are a policy expression that includes an AT policy assertion (Line 14) to indicate that a capability of the target service is that it will process messages in a transaction regardless of whether any AtomicTransaction CoordinationContext is sent by the requester.

Lines (20-23) are a WSDL [WSDL 1.1] binding. Line (21) indicates that the policy in Lines (13-16) applies to this binding, specifically indicating that QueryBalance messages are processed in an atomic transaction regardless of whether a requester provides an AtomicTransaction CoordinationContext.

Lines (24-27) are a WSDL [WSDL 1.1] binding. Line (25) indicates that the policy in Lines (9-12) applies to this binding, specifically indicating that an atomic transaction MAY flow inside messages.

6 Transaction Faults

WS-AtomicTransaction faults MUST include as the [action] property the following fault action URI:

```
http://docs.oasis-open.org/ws-tx/wsat/2006/03/fault
```

The faults defined in this section are generated if the condition stated in the preamble is met. Faults are targeted at a destination endpoint according to the fault handling rules defined in [WSADDR].

The definitions of faults in this section use the following properties:

[Code] The fault code.

[Subcode] The fault subcode.

[Reason] The English language reason element.

[Detail] The detail element. If absent, no detail element is defined for the fault.

For SOAP 1.2, the [Code] property MUST be either "Sender" or "Receiver". These properties are serialized into text XML as follows:

SOAP Version	Sender	Receiver
SOAP 1.2	S:Sender	S:Receiver

The properties above bind to a SOAP 1.2 fault as follows:

```
<S:Envelope>
 <S:Header>
   <wsa:Action>
      http://docs.oasis-open.org/ws-tx/wsat/2006/03/fault
   </wsa:Action>
   <!-- Headers elided for clarity.  -->
 </S:Header>
 <S:Body>
  <S:Fault>
   <S:Code>
     <S:Value>[Code]</S:Value>
     <S:Subcode>
      <S:Value>[Subcode]</S:Value>
     </S:Subcode>
   </S:Code>
   <S:Reason>
     <S:Text xml:lang="en">[Reason]</S:Text>
   </S:Reason>
   <S:Detail>
     [Detail]
     ...
   </S:Detail>
  </S:Fault>
 </S:Body>
</S:Envelope>
```

The properties bind to a SOAP 1.1 fault as follows:

```
<S11:Envelope>
```

```
 <S11:Body>
  <S11:Fault>
   <faultcode>[Subcode]</faultcode>
   <faultstring xml:lang="en">[Reason]</faultstring>
  </S11:Fault>
 </S11:Body>
</S11:Envelope>
```

6.1 InconsistentInternalState

This fault is sent by a participant to indicate that it cannot fulfill its obligations. This indicates a global consistency failure and is an unrecoverable condition.

Properties:

[Code] Sender

[Subcode] wsat:InconsistentInternalState

[Reason] A global consistency failure has occurred. This is an unrecoverable condition.

[Detail] unspecified

7 Security Model

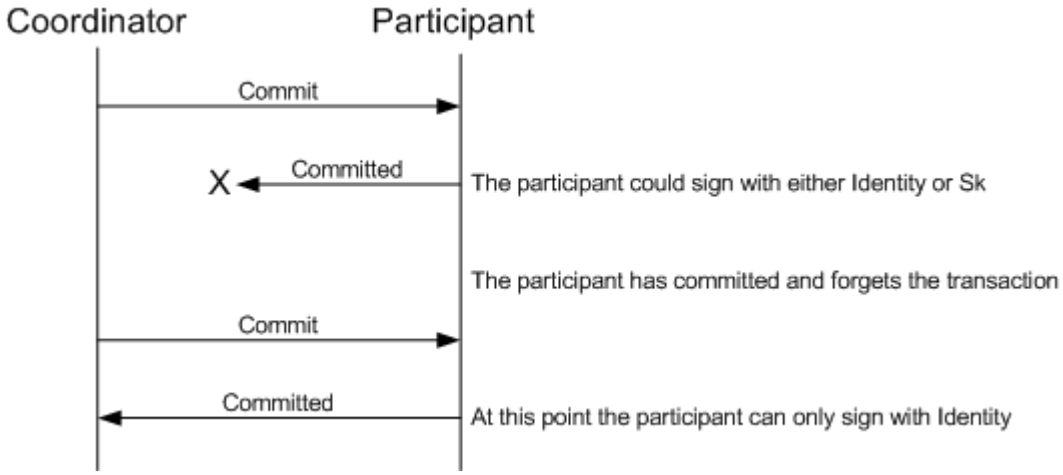
The security model for atomic transactions builds on the model defined in WS-Coordination [WSCOOR]. That is, services have policies specifying their requirements and requestors provide claims (either implicit or explicit) and the requisite proof of those claims. Coordination context creation establishes a base secret which can be delegated by the creator as appropriate.

Because atomic transactions represent a specific use case rather than the general nature of coordination contexts, additional aspects of the security model can be specified.

All access to atomic transaction protocol instances is on the basis of identity. The nature of transactions, specifically the uncertainty of systems means that the security context established to register for the protocol instance may not be available for the entire duration of the protocol.

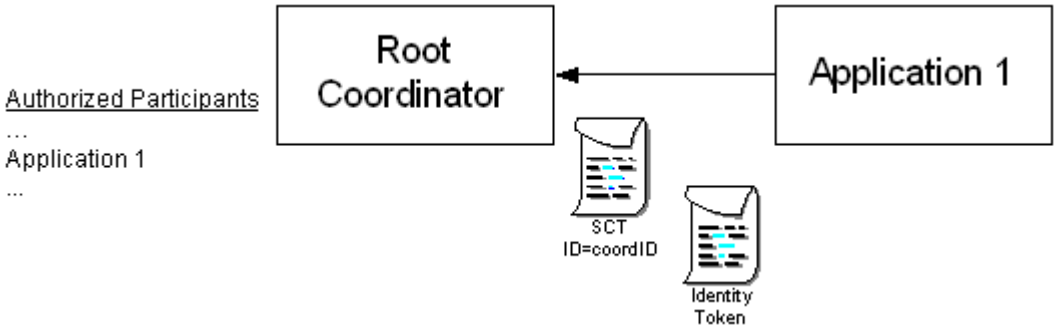
Consider for example the scenarios where a participant has committed its part of the transaction, but for some reason the coordinator never receives acknowledgement of the commit. The result is that when communication is re-established in the future, the coordinator will attempt to confirm the commit status of the participant, but the participant, having committed the transaction and forgotten all information associated with it, no longer has access to the special keys associated with the token.

The participant can only prove its identity to the coordinator when it indicates that the specified transaction is not in its log and assumed committed. This is illustrated in the figure below:



There are, of course, techniques to mitigate this situation but such options will not always be successful. Consequently, when dealing with atomic transactions, it is critical that identity claims always be proven to ensure that correct access control is maintained by coordinators.

There is still value in coordination context-specific tokens because they offer a bootstrap mechanism so that all participants need not be pre-authorized. As well, it provides additional security because only those instances of an identity with access to the token will be able to securely interact with the coordinator (limiting privileges strategy). This is illustrated in the figure below:



403

404 The "list" of authorized participants ensures that application messages having a coordination context are
405 properly authorized since altering the coordination context ID will not provide additional access unless (1)
406 the bootstrap key is provided, or (2) the requestor is on the authorized participant "list" of identities.

8 Security Considerations

It is strongly RECOMMENDED that the communication between services be secured using the mechanisms described in WS-Security [WSSec]. In order to properly secure messages, the body and all relevant headers need to be included in the signature. Specifically, the `<wscoor:CoordinationContext>` header needs to be signed with the body and other key message headers in order to "bind" the two together.

In the event that a participant communicates frequently with a coordinator, it is RECOMMENDED that a security context be established using the mechanisms described in WS-Trust [WSTrust] and WS-SecureConversation [WSSecConv] allowing for potentially more efficient means of authentication.

It is common for communication with coordinators to exchange multiple messages. As a result, the usage profile is such that it is susceptible to key attacks. For this reason it is strongly RECOMMENDED that the keys be changed frequently. This "re-keying" can be effected a number of ways. The following list outlines four common techniques:

- Attaching a nonce to each message and using it in a derived key function with the shared secret
- Using a derived key sequence and switch "generations"
- Closing and re-establishing a security context (not possible for delegated keys)
- Exchanging new secrets between the parties (not possible for delegated keys)

It should be noted that the mechanisms listed above are independent of the SCT and secret returned when the coordination context is created. That is, the keys used to secure the channel may be independent of the key used to prove the right to register with the activity.

The security context MAY be re-established using the mechanisms described in WS-Trust [WSTrust] and WS-SecureConversation [WSSecConv]. Similarly, secrets can be exchanged using the mechanisms described in WS-Trust. Note, however, that the current shared secret SHOULD NOT be used to encrypt the new shared secret. Derived keys, the preferred solution from this list, can be specified using the mechanisms described in WS-SecureConversation.

The following list summarizes common classes of attacks that apply to this protocol and identifies the mechanism to prevent/mitigate the attacks:

- **Message alteration** – Alteration is prevented by including signatures of the message information using WS-Security [WSSec].
- **Message disclosure** – Confidentiality is preserved by encrypting sensitive data using WS-Security.
- **Key integrity** – Key integrity is maintained by using the strongest algorithms possible (by comparing secured policies – see WS-Policy [WSPOLICY] and WS-SecurityPolicy [WSSecPolicy]).
- **Authentication** – Authentication is established using the mechanisms described in WS-Security and WS-Trust [WSTrust]. Each message is authenticated using the mechanisms described in WS-Security [WSSec].
- **Accountability** – Accountability is a function of the type of and string of the key and algorithms being used. In many cases, a strong symmetric key provides sufficient accountability. However, in some environments, strong PKI signatures are required.

- **Availability** – Many services are subject to a variety of availability attacks. Replay is a common attack and it is RECOMMENDED that this be addressed as described in the next bullet. Other attacks, such as network-level denial of service attacks are harder to avoid and are outside the scope of this specification. That said, care should be taken to ensure that minimal processing be performed prior to any authenticating sequences.

- **Replay** – Messages may be replayed for a variety of reasons. To detect and eliminate this attack, mechanisms should be used to identify replayed messages such as the timestamp/nonce outlined in WS-Security [WSSec]. Alternatively, and optionally, other technologies, such as sequencing, can also be used to prevent replay of application messages.

9 Use of WS-Addressing Headers

The messages defined in WS-AtomicTransaction can be classified into two types:

- Notification messages: **Commit**, **Rollback**, **Committed**, **Aborted**, **Prepare**, **Prepared**, **ReadOnly** and **Replay**.
- Fault messages

Notification messages follow the standard "one way" pattern as defined in WS-Addressing. There are two types of notification messages:

- A notification message is a terminal message when it indicates the end of a coordinator/participant relationship. **Committed**, **Aborted** and **ReadOnly** are terminal messages.
- A notification message is a non-terminal message when it does not indicate the end of a coordinator/participant relationship. **Commit**, **Rollback**, **Prepare**, **Prepared** and **Replay** are non-terminal messages.

The following statements define addressing interoperability requirements for the WS-AtomicTransaction message types:

Non-terminal notification messages

- MUST include a wsa:ReplyTo header

Terminal notification messages

- SHOULD NOT include a wsa:ReplyTo header

Fault messages

- MUST include a wsa:RelatesTo header, specifying the MessageID from the Notification message that generated the fault condition.

Notification messages are addressed by both coordinators and participants using the Endpoint References initially obtained during the Register-RegisterResponse exchange. If a wsa:ReplyTo header is present in a notification message it MAY be used by the recipient, for example in cases where a Coordinator or Participant has forgotten a transaction that is completed and needs to respond to a resent protocol message. Permanent loss of connectivity between a coordinator and a participant in an in-doubt state can result in data corruption.

If a wsa:FaultTo header is present on a message that generates a fault condition, then it MUST be used by the recipient as the destination for any fault. Otherwise, fault messages MAY be addressed by both coordinators and participants using the Endpoint References initially obtained during the Register-RegisterResponse exchange.

All messages are delivered using connections initiated by the sender. Endpoint References MUST contain physical addresses and MUST NOT use the well-known "anonymous" endpoint defined in WS-Addressing.

10 State Tables

The following state tables specify the behavior of coordinators and participants when presented with protocol messages or internal events. These tables present the view of a coordinator or participant with respect to a single partner. A coordinator with multiple participants can be understood as a collection of independent coordinator state machines.

Each cell in the tables uses the following convention:

Legend
Action to take
Next state

Each state supports a number of possible events. Expected events are processed by taking the prescribed action and transitioning to the next state. Unexpected protocol messages will result in a fault message, with a standard fault code such as Invalid State or Inconsistent Internal State. Events that may not occur in a given state are labeled as N/A.

Atomic Transaction 2PC protocol (Coordinator View)							
Inbound Events	**States**						
	None	**Active**	**Preparing**	**Prepared**	**PreparedSuccess**	**Committing**	**Aborting**
Register	*Invalid State* None	*Send RegisterResponse* Active	*Durable: Invalid State* Aborting *Volatile: Send RegisterResponse* Active	*N/A*	*Invalid State* PreparedSuccess	*Invalid State* Committing	*Invalid State* Aborting
Prepared	*Durable: Send Rollback* *Volatile: Invalid State* None	*Invalid State* Aborting	*Record Vote* Preparing	*N/A*	*Ignore* PreparedSuccess	*Resend Commit* Committing	*Resend Rollback, and Forget* Aborting
ReadOnly	*Ignore* None	*Forget* Active	*Forget* Preparing	*N/A*	*Invalid State* PreparedSuccess	*Invalid State* Committing	*Forget* Aborting
Aborted	*Ignore* None	*Forget* Aborting	*Forget* Aborting	*N/A*	*Invalid State* PreparedSuccess	*Invalid State* Committing	*Forget* Aborting
Committed	*Ignore* None	*Invalid State* Aborting	*Invalid State* Aborting	*N/A*	*Invalid State* PreparedSuccess	*Forget* Committing	*Invalid State* Aborting
Replay	*Durable: Send Rollback* *Volatile: Invalid State* None	*Send Rollback* Aborting	*Send Rollback* Aborting	*N/A*	*Ignore* PreparedSuccess	*Send Commit* Committing	*Send Rollback* Aborting
Internal Events							
User Commit	*Return Aborted* None	*Send Prepare* Preparing	*Ignore* Preparing	*N/A*	*Ignore* Prepared Success	*Return Committed* Committing	*Return Aborted* Aborting
User Rollback	*Return Aborted* None	*Send Rollback* Aborting	*Send Rollback* Aborting	*N/A*	*Invalid State* PreparedSuccess	*Invalid State* Committing	*Return Aborted* Aborting
Expires Times Out	*N/A*	*Send Rollback* Aborting	*Send Rollback* Aborting	*N/A*	*Ignore* PreparedSuccess	*Ignore* Committing	*Ignore* Aborting
Comms Times Out	*N/A*	*N/A*	*Resend Prepare* Preparing	*N/A*	*N/A*	*Resend Commit* Committing	*N/A*
Commit Decision	*N/A*	*N/A*	*Record Outcome* Prepared Success	*N/A*	*N/A*	*N/A*	*N/A*
Write Done	*N/A*	*N/A*	*N/A*	*N/A*	*Send Commit* Committing	*N/A*	*N/A*
Write Failed	*N/A*	*N/A*	*N/A*	*N/A*	*Send Rollback* Aborting	*N/A*	*N/A*
All Forgotten	*N/A*	Active	None	*N/A*	*N/A*	None	None

Notes:

1. Transitions with a “N/A” as their action are inexpressible. A TM should view these transitions as serious internal consistency issues, and probably fatal.
2. Internal events are those that are created either within a TM itself, or on its local system.

“Forget” implies that the subordinate’s is participation is removed from the coordinator (if necessary), and otherwise the message is ignored

Atomic Transaction 2PC Protocol (Participant View)							
Inbound Events	**States**						
	None	**Active**	**Preparing**	**Prepared**	**PreparedSuccess**	**Committing**	**Aborting**
Register Response	*Register Subordinate* Active	*Ignore* Active	*Ignore* Preparing	*Ignore* Prepared	*Ignore* PreparedSuccess	*Ignore* Committing	*Ignore* Aborting
Prepare	*Send Aborted* None	*Gather Vote Decision* Preparing	*Ignore* Preparing	*Ignore* Prepared	*Resend Prepared* PreparedSuccess	*Ignore* Committing	*Resend Aborted, and Forget* Aborting
Commit	*Send Committed* None	*Invalid State* Aborting	*Invalid State* Aborting	*Invalid State* Aborting	*Initiate Commit Decision* Committing	*Ignore* Committing	*InconsistentInternalState* Aborting
Rollback	*Send Aborted* None	*Initiate Rollback, Send Aborted, and Forget* Aborting	*Initiate Rollback, Send Aborted, and Forget* Aborting	*Initiate Rollback, Send Aborted, and Forget* Aborting	*Initiate Rollback, Send Aborted, and Forget* Aborting	*InconsistentInternalState* Committing	*Send Aborted, and Forget* Aborting
Internal Events							
Expires Times Out	*N/A*	*Send Aborted* Aborting	*Send Aborted* Aborting	*Ignore* Prepared	*Ignore* PreparedSuccess	*Ignore* Committing	*Ignore* Aborting
Comms Times Out	*N/A*	*N/A*	*N/A*	*N/A*	*Resend Prepared* PreparedSuccess	*N/A*	*N/A*
Commit Decision	*N/A*	*N/A*	*Record Commit* Prepared	*N/A*	*N/A*	*Send Committed and Forget* Committing	*N/A*
Rollback Decision	*N/A*	*N/A*	*Send Aborted* Aborting	*N/A*	*N/A*	*N/A*	*N/A*
Write Done	*N/A*	*N/A*	*N/A*	*Send Prepared* PreparedSuccess	*N/A*	*N/A*	*N/A*
Write Failed	*N/A*	*N/A*	*N/A*	*Initiate Rollback, Send Aborted, and Forget* Aborting	*N/A*	*N/A*	*N/A*
All Forgotten	None	*N/A*	*Send ReadOnly* None	*N/A*	*N/A*	None	None

Notes:

1. Transitions with a “N/A” as their action are inexpressible. A TM should view these transitions as serious internal consistency issues, and probably fatal.
2. Internal events are those that are created either within a TM itself, or on its local system.

Appendix A. Acknowledgements

This document is based on initial contributions to the OASIS WS-TX Technical Committee by the following authors: Luis Felipe Cabrera, Microsoft, George Copeland, Microsoft, Max Feingold, Microsoft, Robert W Freund, Hitachi, Tom Freund, IBM, Sean Joyce, IONA, Johannes Klein, Microsoft, David Langworthy, Microsoft, Mark Little, Arjuna Technologies, Frank Leymann, IBM, Eric Newcomer, IONA, David Orchard, BEA Systems, Ian Robinson, IBM, Tony Storey, IBM, Satish Thatte, Microsoft.

The following individuals have provided invaluable input into the initial contribution: Francisco Curbera, IBM, Doug Davis, IBM, Gert Drapers, Microsoft, Don Ferguson, IBM, Kirill Gavrylyuk, Microsoft, Dan House, IBM, Oisin Hurley, IONA, Thomas Mikalsen, IBM, Jagan Peri, Microsoft, John Shewchuk, Microsoft, Stefan Tai, IBM.

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

Appendix B. Revision History

Revision	yy-mm-dd	Editor	Changes Made
01	05-11-22	Mark Little	Initial Working Draft
01	05-11-23	Andrew Wilkinson	Initial Working Draft
02	06-02-12	Mark Little	Updated for issue i017
03	06-03-02	Andrew Wilkinson	Updated for issue 015
04	06-03-10	Andrew Wilkinson	Updated for issue 009
cd-01	06-03-15	Andrew Wilkinson	Updates to produce CD-01