Style Definition: Normal: Font: (Asian) MS Mincho

Web Services Security
Kerberos Token Profile 1.1

Draft – 11 October 2005

Deleted: OASIS Public Review
Deleted: 28
Deleted: June

OASIS identifier:
{product-productVersion-artifactType-stage-descriptiveName-revision.form (Word) (PDF) (HTML)}

Location:
http://docs.oasis-open.org/wss/2005/xx/wss-v1.1-spec-draft-KerberosTokenProfile-01

Deleted: http://docs.oasis-open.org/wss/2005/xx/wss-v1.1-spec-pr-

Technical Commitee:

Formatted: Default Paragraph Font

Web Service Security (WSS)

Formatted: Indent: Left: 0"

Chairs:

Kelvin Lawrence, IBM

Formatted: Indent: Left: 0", Space Before: 6 pt

Chris Kaler, Microsoft

Formatted: Space Before: 6 pt

Editors:

Anthony Nadalin, IBM

Formatted: Indent: Left: 0", Space Before: 6 pt

Chris Kaler, Microsoft

Ronald Monzillo, Sun

Formatted: Space Before: 6 pt

Phillip Hallam-Baker, Verisign

Formatted: Indent: Left: 0", Space Before: 6 pt

Abstract:
This document describes how to use Kerberos [Kerb] tickets (specifically the AP-REQ packet) with the WSS: SOAP Message Security [WSS] specification.

Status:
This is an interim draft. Please send comments to the editors.

Committee members should send comments on this specification to the wss@lists.oasis-open.org list. Others should subscribe to and send comments to the wss-comment@lists.oasis-open.org list. To subscribe, visit http://lists.oasis-open.org/ob/adm.pl.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing

Deleted: 28
Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasis-open.org/who/intellectualproperty.shtml).

Copyright © OASIS Open 2002-2005. All Rights Reserved.

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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

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 Executive Director.

Copyright © The Organization for the Advancement of Structured Information Standards [OASIS] 2002-2005. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself must not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assignees.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

Deleted: does

Deleted: s

Deleted: 28

Deleted: June

Table of Contents

Deleted: 1 . Introduction . 4¶
2 . Notations and Terminology . 5¶
2.1 Notational Conventions . 5¶
2.2 Namespaces . 5¶
2.3 Terminology . 6¶
3 . Usage . 7¶
3.1 Processing Model . 7¶
3.2 Attaching Security Tokens . 7¶
3.3 Identifying and Referencing Kerberos Tokens . 8¶
3.4 Authentication . 9¶
3.5 Encryption . 10¶
3.6 Principal Name . 10¶
3.7 Error Codes . 10¶
4 . Threat Model and Countermeasures . 11¶
5 . References . 12¶
Appendix A. Acknowledgments . 13¶
Appendix B. Revision History . 16¶

Deleted: 28

Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

1 Introduction

This specification describes the use of Kerberos [Kerb] tokens with respect to the WSS: SOAP Message Security specification [WSS].

Specifically, this document defines how to encode Kerberos tickets and attach them to SOAP messages. As well, it specifies how to add signatures and encryption to the SOAP message, in accordance with WSS: SOAP Message Security, which uses and references the Kerberos tokens.

For interoperability concerns, and for some security concerns, the specification is limited to using the AP-REQ packet (service ticket and authenticator) defined by Kerberos as the Kerberos token. This allows a service to authenticate the ticket and interoperate with existing Kerberos implementations.

It should be noted that how the AP-REQ is obtained is out of scope of this specification as are scenarios involving other ticket types and user-to-user interactions.

Note that Sections 2.1, 2.2, all of 3, and indicated parts of 6 are normative. All other sections are non-normative.

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Deleted: 28
Deleted: June

2 Notations and Terminology

This section specifies the notations, namespaces, and terminology used in this specification.

2.1 Notational Conventions

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 [2119].

Namespace URIs (of the general form "some-URI") represent some application-dependent or context-dependent URI as defined in RFC2396 [URI].

This specification is designed to work with the general SOAP [S11, S12] message structure and message processing model, and should be applicable to any version of SOAP. The current SOAP 1.2 namespace URI is used herein to provide detailed examples, but there is no intention to limit the applicability of this specification to a single version of SOAP.

2.2 Namespaces

The XML namespace [XML-ns] URIs that MUST be used by implementations of this specification are as follows (note that different elements in this specification are from different namespaces):

```
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd
http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-
secext-1.1.xsd
```

Note that this specification does not introduce new schema elements.

The following namespaces are used in this document:

Prefix	Namespace
S11	http://schemas.xmlsoap.org/soap/envelope/
S12	http://www.w3.org/2003/05/soap-envelope
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

Deleted: 28

Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

wsse11	http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-secext-1.1.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc#

The URLs provided for the *wsse* and *wsu* namespaces can be used to obtain the schema files. URI fragments defined in this specification are relative to the following base URI unless otherwise specified:

http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1

2.3 Terminology

Readers are presumed to be familiar with the terms in the Internet Security Glossary [ISG].

This specification employs the terminology defined in the WSS: SOAP Message Security Core Specification [WSS].

The following (non-normative) table defines additional acronyms and abbreviations for this document.

Term	**Definition**
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
URI	Uniform Resource Identifier
XML	Extensible Markup Language

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Deleted: 28
Deleted: June

3 Usage

This section describes the profile (specific mechanisms and procedures) for the Kerberos binding of WSS: SOAP Message Security.

Identification: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1

3.1 Processing Model

The processing model for WSS: SOAP Message Security with Kerberos tokens is no different from that of WSS: SOAP Message Security with other token formats as described in WSS: SOAP Message Security.

3.2 Attaching Security Tokens

Kerberos tokens are attached to SOAP messages using WSS: SOAP Message Security by using the <wsse:BinarySecurityToken> described in WSS: SOAP Message Security. When using this element, the *@ValueType* attribute MUST be specified. This specification defines four values for this token as defined in the table below:

URI	Description
http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ1510	Kerberos v5 AP-REQ as defined in RFC1510. This ValueType is used when the ticket is an AP Request per RFC1510.
http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	A GSS wrapped Kerberos v5 AP-REQ as defined in the GSSAPI specification. This ValueType is used when the ticket is an AP Request (ST + Authenticator) per RFC1510.
http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ4120	Kerberos v5 AP-REQ as defined in RFC4120. This ValueType is used when the ticket is an AP Request per RFC4120
http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ4120	A GSS wrapped Kerberos v5 AP-REQ as defined in the GSSAPI specification. This ValueType is used when the ticket is an AP Request (ST + Authenticator) per RFC4120.

It should be noted that the URIs in the table above also serve as the official URIs identifying the Kerberos tokens defined in this specification.

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Formatted: Font: (Default) Arial
Formatted: Font: Not Bold
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Courier New
Deleted: two
Formatted: Font: (Default) Courier New
Formatted: Font: (Default) Arial
Formatted: Normal (Web)
Formatted: Font: (Default) Courier New
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ
Deleted: Kerberos v5 AP-REQ as defined in the Kerberos specification. This ValueType is used when the ticket is an AP Request
Formatted: Font: (Default) Courier New
Formatted: Font: (Default) Arial
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ
Formatted: Font: (Default) Courier New
Deleted: A GSS wrapped Kerberos v5 AP-REQ as defined in the GSSAPI specification. This ValueType is used when the ticket is an AP Request (ST + Authenticator).
Formatted: Font: (Default) Courier New
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Courier New
Formatted: Font: (Default) Courier New
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Courier New
Formatted: Font: (Default) Arial
Deleted: s
Deleted: 28
Deleted: June

Both token types defined in this section use the type 0x8003 defined in RFC1964 for the checksum field of the authenticator inside the AP_REQ.

The octet sequence of either the GSS wrapped AP_REQ or an unwrapped AP_REQ is encoded using the indicated encoding (e.g. base 64) and the result is placed inside of the `<wsse:BinarySecurityToken>` element.

The following example illustrates a SOAP message with a Kerberos token.

```
<S11:Envelope xmlns:S11="...">
    <S11:Header>
        <wsse:Security xmlns:wsse="...">
            <wsse:BinarySecurityToken EncodingType="http://docs.
               oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-
1.1#Kerberosv5_AP_REQ" wsu:Id="MyToken">boIBxDCCAcCgAwIBBaEDAgEOogcD...
            </wsse:BinarySecurityToken>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
</S11:Envelope>
```

Deleted: the
Formatted: Font: (Default) Arial
Deleted: Kerberos ticket
Deleted: the Kerberos ticket
Deleted: (e.g. AP-REQ)
Deleted: algorithm
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial

Deleted: <wsse:BinarySecurity Token ¶
xmlns:wsse="... " ¶
wsu:Id="myToken"¶
ValueType="...#Kerberosv5_AP _REQ"¶
EncodingType="...#Base64Bina ry">¶
MIIEZzCCA9CgAwIBAgIQEmtJZc0. ..¶
</wsse:BinarySecurityToken>

3.3 Identifying and Referencing Kerberos Tokens

A Kerberos Token is referenced by means of the `<wsse:SecurityTokenReference>` element. This mechanism, defined in WSS: SOAP Message Security, provides different referencing mechanisms. The following list identifies the supported and unsupported mechanisms:

The *wsu:Id* MAY be specified on the `<wsse:BinarySecurityToken>` element allowing the token to be directly referenced.

A `<wsse:KeyIdentifier>` element MAY be used which specifies the identifier for the Kerberos ticket. This value is computed as the SHA1 of the pre-encoded octets that were used to form the contents of the `<wsse:BinarySecurityToken>` element. The `<wsse:KeyIdentifier>` element contains the encoded form the of the KeyIdentifier which is defined as the base64 encoding of the SHA1 result.

Key Name references MUST NOT be used.

When a Kerberos Token is referenced using `<wsse:SecurityTokenReference>` the *@ValueType* attribute is not required. If specified, the URI listed above as Kerberos token type MUST be specified.

The `<wsse:SecurityTokenReference>` element from which the reference is made contains the `<wsse:KeyIdentifier>` element. The `<wsse:KeyIdentifier>` element MUST have a `ValueType` attribute on the `<wsse:KeyIdentifier>` element with the value `#Kerberosv5APREQSHA1` and its contents MUST be the SHA1 of GSS wrapped or unwrapped

Formatted: Font: (Default) Courier New
Deleted: 28
Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

AP-REQ, as appropriate, encoded as per the `<wsse:KeyIdentifier>` element's `EncodingType` attribute.

Reference Identifier	**ValueType URI**	Description
Kerberos v5 AP-REQ	#Kerberosv5APREQSHA1	SHA1 of the v5 AP-REQ octets, either GSS wrapped Kerberos AP-REQ or just the Kerberos AP-REQ.

The following example illustrates using ID references to a Kerberos token:

```
<S11:Envelope xmlns:S11="...">
    <S11:Header>
        <wsse:Security xmlns:wsse="...">
            <wsse:BinarySecurityToken EncodingType="http://docs.
oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary" ValueType=http://docs.oasis-
open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-
1.1#Kerberosv5_AP_REQ wsu:Id="MyToken">
                boIBxDCCAcCgAwIBBaEDAgEOogcD...
            </wsse:BinarySecurityToken>
            ...
               <wsse:SecurityTokenReference>
                   <wsse:Reference URI="#MyToken"
ValueType="http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-
kerberos-token-profile-1.1#Kerberosv5APREQSHA1">
                   </wsse:Reference>
               </wsse:SecurityTokenReference>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
</S11:Envelope>
```

Deleted: <wsse:BinarySecurity Token ¶ xmlns:wsse="... " ¶ wsu:Id="myToken"¶ ValueType="...#Kerberosv5_AP _REQ"¶ EncodingType="...#Base64Bina ry">¶ MIIEZzCCA9CgAwIBAgIQEmtJZc0. ..¶ </wsse:BinarySecurityToken>

Deleted: <wsse:SecurityTokenR eference>¶ <wsse:Reference URI="#myToken"/>¶ </wsse:SecurityTokenReferenc e>

The AP-REQ packet is included in the initial message to the service, but need not be attached to subsequent messages exchanged between the involved parties. Consequently, the KeyIdentifier reference mechanism SHOULD be used on subsequent exchanges as illustrated in the example below:

```
<S11:Envelope xmlns:S11="...">
    <S11:Header>
        <wsse:Security xmlns:wsse="...">
            ...
               <wsse:SecurityTokenReference>
                 <wsse:KeyIdentifier ValueType="http://docs.oasis-
open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-
1.1#Kerberosv5APREQSHA1">GbsDt+WmD9XlnUUWbY/nhBveW8I=
```

Deleted: 28

Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

```
                </wsse:KeyIdentifier>
            </wsse:SecurityTokenReference>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
</S11:Envelope>
```

Deleted: <wsse:SecurityTokenReference <wsse:KeyIdentifier ValueType="...#Kerberosv5APREQSHA1">¶ EZzCCA9CgAwIB...¶ <wsse:KeyIdentifier>¶ </wsse:SecurityTokenReference>

3.4 Authentication

When a Kerberos ticket is referenced as a signature key, the signature algorithm [DSIG] MUST be a hashed message authentication code.

When a Kerberos ticket is referenced as an encryption key, the encryption algorithm MUST be a symmetric encryption algorithm.

The value of the signature or encryption key is constructed from the value of the Kerberos sub-key when it is present in the authenticator or a session key from the ticket if the sub-key is absent, either by using the Kerberos sub-key or session key directly or using a key derived from that key using a mechanism agreed to by the communicating parties.

3.5 Encryption

When a Kerberos ticket is referenced as an encryption key, the encryption algorithm MUST be a symmetric encryption algorithm.

The value of the signature or encryption key is constructed from the value of the Kerberos sub-key when it is present in the authenticator or a session key from the ticket if the sub-key is absent, either by using the Kerberos sub-key or session key directly or using a key derived from that key using a mechanism agreed to by the communicating parties..

3.6 Principal Name

Kerberos principal name definition and mapping of non-Kerberos names to Kerberos V principal names are out of scope of this document.

3.7 Error Codes

When using Kerberos tokens, it is RECOMMENDED to use the error codes defined in the WSS: SOAP Message Security specification. However, implementations MAY use custom errors, defined in private namespaces if they desire. Care should be taken not to introduce security vulnerabilities in the errors returned.

Deleted: 28

Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

4 Threat Model and Countermeasures

The use of Kerberos assertion tokens with WSS: SOAP Message Security introduces no new message-level threats beyond those identified for Kerberos itself or by WSS: SOAP Message Security with other types of security tokens.

One potential threat is that of key re-use. The mechanisms described in WSS: SOAP Message Security can be used to prevent replay of the message; however, it is possible that for some service scopes, there are host security concerns of key hijacking within a Kerberos infrastructure. The use of the AP-REQ and its associated authenticator and sequencer mitigate this threat.

Message alteration and eavesdropping can be addressed by using the integrity and confidentiality mechanisms described in WSS: SOAP Message Security. Replay attacks can be addressed by using message timestamps and caching, as well as other application-specific tracking mechanisms. For Kerberos tokens ownership is verified by use of keys, so man-in-the-middle attacks are generally mitigated.

It is strongly recommended that GSS wrapped AP-REQ be used or that unwrapped AP-REQ be combined with timestamp be used to prevent replay attack.

It is strongly recommended that all relevant and immutable message data be signed to prevent replay attacks.

It should be noted that transport-level security MAY be used to protect the message and the security token in cases where neither a wrapped AP-REQ nor an unwrapped AP-REQ combined with timestamp and signature are being used.

Formatted: Font: Arial

Deleted: It should be noted that transport-level security MAY be used to protect the message and the security token if either a wrapped AP-REQ or that unwrapped AP-REQ be combined with timestamp and signature are not being used.

Formatted: Font: Arial

Deleted: 28

Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

5 References

The following are normative references

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

[Kerb] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, September 1993, http://www.ietf.org/rfc/rfc1510.txt .

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

[S11] W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.

[S12] W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging Framework", 23 June 2003.

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe Systems, January 2005.

[WSS] A. Nadalin et al., Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf.

The following are non-normative references

[ISG] Informational RFC 2828, "Internet Security Glossary," May 2000.

[XML-ns] W3C Recommendation, "Namespaces in XML," 14 January 1999.

[DSIG] D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002. http://www.w3.org/TR/xmldsig-core/.

Deleted: [WSS] . A. Nadalin et al., Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), OASIS Standard 200401, March 2004, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.¶

Deleted: 28

Deleted: June

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Appendix A. Acknowledgments

Current Contributors:

Michael	Hu	Actional
Maneesh	Sahu	Actional
Duane	Nickull	Adobe Systems
Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Laboratory
Hal	Lockhart	BEA Systems
Denis	Pilipchuk	BEA Systems
Corinna	Witt	BEA Systems
Steve	Anderson	BMC Software
Rich	Levinson	Computer Associates
Thomas	DeMartini	ContentGuard
Merlin	Hughes	Cybertrust
Dale	Moberg	Cyclone Commerce
Rich	Salz	Datapower
Sam	Wei	EMC
Dana S.	Kaufman	Forum Systems
Toshihiro	Nishimura	Fujitsu
Kefeng	Chen	GeoTrust
Irving	Reid	Hewlett-Packard
Kojiro	Nakayama	Hitachi
Paula	Austel	IBM
Derek	Fu	IBM
Maryann	Hondo	IBM
Kelvin	Lawrence	IBM
Michael	McIntosh	IBM
Anthony	Nadalin	IBM
Nataraj	Nagaratnam	IBM
Bruce	Rich	IBM
Ron	Williams	IBM
Don	Flinn	Individual
Kate	Cherry	Lockheed Martin
Paul	Cotton	Microsoft
Vijay	Gajjala	Microsoft
Martin	Gudgin	Microsoft
Chris	Kaler	Microsoft
Frederick	Hirsch	Nokia
Abbie	Barbir	Nortel
Prateek	Mishra	Oracle
Vamsi	Motukuru	Oracle
Ramana	Turlapi	Oracle
Ben	Hammond	RSA Security
Rob	Philpott	RSA Security
Blake	Dournaee	Sarvega
Sundeep	Peechu	Sarvega
Coumara	Radja	Sarvega
Pete	Wenzel	SeeBeyon
Manveen	Kaur	Sun Microsystem

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Deleted: This specification wa ... [1]
Formatted ... [2]
Formatted Table ... [3]
Formatted ... [4]
Formatted ... [5]
Formatted ... [6]
Formatted ... [7]
Formatted ... [8]
Formatted ... [9]
Formatted ... [10]
Formatted ... [11]
Formatted ... [12]
Formatted ... [13]
Formatted ... [14]
Formatted ... [15]
Formatted ... [16]
Formatted ... [17]
Formatted ... [18]
Formatted ... [19]
Formatted ... [20]
Formatted ... [21]
Formatted ... [22]
Formatted ... [23]
Formatted ... [24]
Formatted ... [25]
Formatted ... [26]
Formatted ... [27]
Formatted ... [28]
Formatted ... [29]
Formatted ... [30]
Formatted ... [31]
Formatted ... [32]
Formatted ... [33]
Formatted ... [34]
Formatted ... [35]
Formatted ... [36]
Formatted ... [37]
Formatted ... [38]
Formatted ... [39]
Formatted ... [40]
Formatted ... [41]
Formatted ... [42]
Formatted ... [43]
Formatted ... [44]
Formatted ... [45]
Formatted ... [46]
Formatted ... [47]
Formatted ... [48]
Formatted ... [49]
Deleted: 28…June ... [50]

Ronald	Monzillo	Sun Microsystem
Jan	Alexander	Systine
Symon	Chang	TIBCO Softwar
John	Weiland	US Nav
Hans	Granqvist	VeriSig
Phillip	Hallam-Baker	VeriSig
Hemma	Prafullchandra	VeriSign

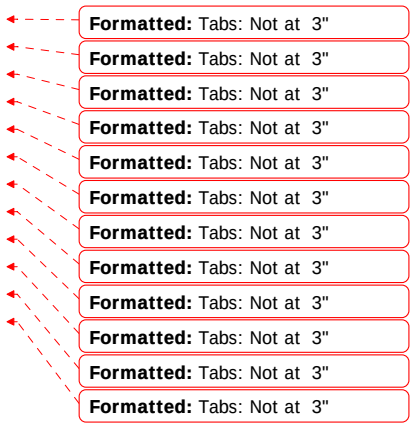
Previous Contributors:

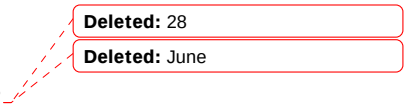
Pete	Dapkus	BEA
Guillrmo	Lao	ContentGuard
T	Pannu	ContentGuard
Xi	Wang	ContentGuard
Shan	Sharp	Cyclone Commerce
Gansh	Vaideeswaran	Documentum
Ti	Moses	Entrust
Carolna	Canales-Valenzuela	Ericsson
To	Rutt	Fujitsu
Yutaa	Kudo	Hitachi
Jaso	Rouault	HP
Bo	Blakley	IBM
Joe	Farrell	IBM
Satohi	Hada	IBM
Hirosi	Maruyama	IBM
Davi	Melgar	IBM
Ken	Tamura	IBM
Waye	Vicknair	IBM
Phi	Griffin	Individual
Mar	Hayes	Individual
Joh	Hughes	Individual
Pete	Rostin	Individual
Davaum	Srinivas	Individual
Bo	Morgan	Individual/Internet2
Bo	Atkinson	Microsoft
Keit	Ballinger	Microsoft
Alle	Brown	Microsoft
Giovnni	Della-Libera	Microsoft
Ala	Geller	Microsoft
Johanes	Klein	Microsoft
Scott	Konersmann	Microsoft
Chris	Kurt	Microsoft
Brian	LaMacchia	Microsoft
Paul	Leach	Microsoft
John	Manferdelli	Microsoft
John	Shewchuk	Microsoft
Dan	Simon	Microsoft
Hervey	Wilson	Microsoft
Jeff	Hodges	Neustar
Senthil	Sengodan	Nokia
Lloyd	Burch	Novel
Ed	Reed	Novel

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Formatted ... [51]
Formatted ... [52]
Formatted ... [53]
Formatted ... [54]
Formatted ... [55]
Formatted ... [56]
Formatted ... [57]
Formatted ... [58]
Formatted ... [59]
Formatted Table ... [60]
Formatted ... [61]
Formatted ... [62]
Formatted ... [63]
Formatted ... [64]
Formatted ... [65]
Formatted ... [66]
Formatted ... [67]
Formatted ... [68]
Formatted ... [69]
Formatted ... [70]
Formatted ... [71]
Formatted ... [72]
Formatted ... [73]
Formatted ... [74]
Formatted ... [75]
Formatted ... [76]
Formatted ... [77]
Formatted ... [78]
Formatted ... [79]
Formatted ... [80]
Formatted ... [81]
Formatted ... [82]
Formatted ... [83]
Formatted ... [84]
Formatted ... [85]
Formatted ... [86]
Formatted ... [87]
Formatted ... [88]
Formatted ... [89]
Formatted ... [90]
Formatted ... [91]
Formatted ... [92]
Formatted ... [93]
Formatted ... [94]
Formatted ... [95]
Formatted ... [96]
Formatted ... [97]
Formatted ... [98]
Formatted ... [99]
Formatted ... [100]
Formatted ... [101]
Deleted: 28…June ... [102]

Charles	Knouse	Obli
Vipin	Samar	Orace
Jerry	Schwarz	Oracle
Eric	Gravengaard	Reactivity
Andrew	Nash	Reactivity
Stuart	King	Reed Elsevier
Martijn	de Boer	SAP
Jonathan	Tourzan	Sony
Yassir	Elley	Sun
Michael	Nguyen	The IDA of Singapore
Don	Adams	TIBCO
Morten	Jorgensen	Vordel





Copyright © OASIS Open 2002-2005. All Rights Reserved.

337

Deleted: The input specifications for this document were developed as a result of joint work with many individuals and teams, including: Keith Ballinger, Microsoft, Bob Blakley, IBM, Allen Brown, Microsoft, Joel Farrell, IBM, Mark Hayes, VeriSign, Kelvin Lawrence, IBM, Scott Konersmann, Microsoft, David Melgar, IBM, Dan Simon, Microsoft, Wayne Vicknair, IBM.¶

¶

Gene ... [103]

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Appendix B. Revision History

Rev	Date	By Whom	What
WGD 1.1	2005-08-30	Anthony Nadalin	Issue 408, 413, 414, 415, 426
WGD 1.1	2005-10-11	Anthony Nadalin	Issue 404

Copyright © OASIS Open 2002-2005. All Rights Reserved.

Page 14: [1] Deleted **Anthony Nadalin** **9/3/2005 1:59:00 PM**

This specification was developed as a result of joint work of many individuals from the WSS TC.

Page 14: [2] Formatted **Anthony Nadalin** **10/11/2005 9:12:00 AM**

Tabs: Not at 3"

Page 14: [3] Change **Anthony Nadalin** **10/11/2005 9:23:00 AM**

Formatted Table

Page 14: [4] Formatted **Anthony Nadalin** **10/11/2005 9:15:00 AM**

Tabs: Not at 3"

Page 14: [5] Formatted **Anthony Nadalin** **10/11/2005 9:16:00 AM**

Tabs: Not at 3"

Page 14: [6] Formatted **Anthony Nadalin** **10/11/2005 9:16:00 AM**

Tabs: Not at 3"

Page 14: [7] Formatted **Anthony Nadalin** **10/11/2005 9:16:00 AM**

Tabs: Not at 3"

Page 14: [8] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [9] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [10] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [11] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [12] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [13] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [14] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [15] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [16] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [17] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [18] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [19] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [20] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [21] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [22] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [23] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [24] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [25] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [26] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [27] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [28] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [29] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [30] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [31] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [32] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [33] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [34] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [35] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [36] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [37] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [38] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [39] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [40] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 14: [41] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [42] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [43] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [44] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [45] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [46] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [47] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [48] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 14: [49] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 1: [50] Deleted **Anthony Nadalin** **9/3/2005 1:48:00 PM**

28

Page 1: [50] Deleted **Anthony Nadalin** **9/3/2005 1:49:00 PM**

June

Page 15: [51] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [52] Formatted **Anthony Nadalin** **10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [53] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [54] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [55] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [56] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [57] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [58] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Indent: First line: 0"

Page 15: [59] Formatted	**Anthony Nadalin**	**10/11/2005 9:17:00 AM**

Tabs: Not at 3"

Page 15: [60] Change	**Anthony Nadalin**	**9/3/2005 2:15:00 PM**

Formatted Table

Page 15: [61] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [62] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [63] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [64] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [65] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [66] Formatted	**Anthony Nadalin**	**10/11/2005 9:21:00 AM**

Tabs: Not at 3"

Page 15: [67] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 15: [68] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 15: [69] Formatted	Anthony Nadalin	10/11/2005 9:21:00 AM

Tabs: Not at 3"

Page 15: [70] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [71] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [72] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [73] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [74] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [75] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [76] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [77] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [78] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [79] Formatted	Anthony Nadalin	10/11/2005 9:22:00 AM

Tabs: Not at 3"

Page 15: [80] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [81] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [82] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [83] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [84] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [85] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [86] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [87] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [88] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [89] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [90] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [91] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [92] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [93] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [94] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [95] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [96] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [97] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [98] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [99] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [100] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 15: [101] Formatted	**Anthony Nadalin**	**10/11/2005 9:22:00 AM**

Tabs: Not at 3"

Page 1: [102] Deleted	**Anthony Nadalin**	**9/3/2005 1:48:00 PM**

28

Page 1: [102] Deleted	**Anthony Nadalin**	**9/3/2005 1:49:00 PM**

June

Page 17: [103] Deleted	**Anthony Nadalin**	**9/3/2005 1:57:00 PM**

The input specifications for this document were developed as a result of joint work with many individuals and teams, including: Keith Ballinger, Microsoft, Bob Blakley, IBM, Allen Brown, Microsoft, Joel Farrell, IBM, Mark Hayes, VeriSign, Kelvin Lawrence, IBM, Scott Konersmann, Microsoft, David Melgar, IBM, Dan Simon, Microsoft, Wayne Vicknair, IBM.

Gene	**Thurston**	**AmberPoint**

Frank	**Siebenlist**	**Argonne National Lab**

Merlin	**Hughes**	**Baltimore Technologies**

Irving	**Reid**	**Baltimore Technologies**

Peter	**Dapkus**	**BEA**

Hal	**Lockhart**	**BEA**

Steve	**Anderson**	**BMC (Sec)**

Thomas	**DeMartini**	**ContentGuard**

Guillermo	**Lao**	**ContentGuard**

TJ	**Pannu**	**ContentGuard**

Shawn	**Sharp**	**Cyclone Commerce**

Ganesh	**Vaideeswaran**	**Documentum**

Sam	**Wei**	**Documentum**

John	**Hughes**	**Entegrity**

Tim	**Moses**	**Entrust**

Toshihiro	**Nishimura**	**Fujitsu**

Tom	**Rutt**	**Fujitsu**

Yutaka	**Kudo**	**Hitachi**

Jason	**Rouault**	**HP**

Bob	**Blakley**	**IBM**

Joel	**Farrell**	**IBM**

Satoshi	**Hada**	**IBM**

Maryann	**Hondo**	**IBM**

Hiroshi	**Maruyama**	**IBM**

David	**Melgar**	**IBM**

Anthony	**Nadalin**	**IBM**

Nataraj	**Nagaratnam**	**IBM**

Wayne	**Vicknair**	**IBM**

Kelvin	**Lawrence**	**IBM (co-Chair)**

Don	**Flinn**	**Individual**

Bob	**Morgan**	**Individual**

Bob	**Atkinson**	**Microsoft**

Keith	**Ballinger**	**Microsoft**

Allen	**Brown**	**Microsoft**

Paul	**Cotton**	**Microsoft**

Giovanni	**Della-Libera**	**Microsoft**

Vijay	**Gajjala**	**Microsoft**

Johannes	**Klein**	**Microsoft**

Scott	**Konermann**	**Microsoft**

Chris	**Kurt**	**Microsoft**

Brian	**LaMacchia**	**Microsoft**

Paul	**Leach**	**Microsoft**

John	**Manferdell**	**Microsoft**

John	**Shewchuk**	**Microsoft**

Dan	**Simon**	**Microsoft**

Hervey	**Wilson**	**Microsoft**

Chris	**Kaler**	**Microsoft (co-Chair)**

Prateek	**Mishra**	**Netegrity**

Frederick	**Hirsch**	**Nokia**

Senthil	**Sengodan**	**Nokia**

Lloyd	**Burch**	**Novell**

Ed	**Reed**	**Novell**

Charles	**Knouse**	**Oblix**

Vipin	**Samar**	**Oracle**

Jerry	**Schwarz**	**Oracle**

Eric	**Gravengaard**	**Reactivity**

Stuart	**King**	**Reed Elsevier**

Andrew	**Nash**	**RSA Security**

Rob	**Philpott**	**RSA Security**

Peter	**Rostin**	**RSA Security**

Martijn	**de Boer**	**SAP**

Pete	**Wenzel**	**SeeBeyond**

Jonathan	**Tourzan**	**Sony**

Yassir	**Elley**	**Sun Microsystems**

Jeff	**Hodges**	**Sun Microsystems**

Ronald	**Monzillo**	**Sun Microsystems**

Jan	**Alexander**	**Systinet**

Michael	**Nguyen**	**The IDA of Singapore**

Don	**Adams**	**TIBCO**

Symon	**Chang**	**TIBCO**

John	**Weiland**	**US Navy**

Phillip	**Hallam-Baker**	**VeriSign**

Mark	**Hays**	**Verisign**

Hemma	**Prafullchandra**	**VeriSign**

Page 20: [104] Deleted **Anthony Nadalin** **9/3/2005 1:58:00 PM**

Rev	Date	What
01	18-Sep-02	Initial draft based on input documents and editorial review
03	30-Jan-03	Changes in title
04	20-Jan-04	Revise based on comments, switch to new URLs and formats and recent decisions in TC
05	27-Jul-04	Revise based on comments and recent decisions in TC
06	16-May-05	Revise based on comments and recent decisions in TC. Issues 381, 382, 383, 384, 385, 386, 387
07	17-May-05	Formatting Issues
08	14-June-05	Issues 396