



WS-SecurityPolicy 1.2 Errata

Committee Draft 02

12 November 2008

Specification URIs:

This Version:

<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-02.doc>
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-02.pdf>
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-02.html>

Previous Version:

<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-01.doc>
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-01.pdf>
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-01.html>

Latest Approved Version:

N/A

Technical Committee:

OASIS WS-TX TC

Chair(s):

Kelvin Lawrence, IBM
Chris Kaler, Microsoft

Editor(s):

Anthony Nadalin, IBM
Marc Goodner, Microsoft
Abbie Barbir, Nortel

Related work:

This specification errata is related to WS-SecurityPolicy v1.2.

Abstract:

This document lists errata for **WS-SecurityPolicy 1.2 OASIS Standard** [WS-SecurityPolicy] produced by the WS-SX Technical Committee. The standard was approved by the OASIS membership on 1 July 2007.

Status:

This document was last revised or approved by the WS-SX TC on the above date. The level of approval is also listed above. Check the "Latest Approved Version" location noted above for possible later revisions of this document.

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-sx.

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-sx/ipr.php).

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

Notices

Copyright © OASIS Open 2008. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

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 section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, 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 assigns.

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 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

Table of contents

1	Issues Addressed	5
2	Typographical/Editorial Errors	6
2.1	Normative language capitalization changes	6
2.2	Section 1.5 Normative References	11
2.3	Section 2 Security Policy Model.....	11
2.4	Section 4.2.3 ContentEncryptedElements Assertion	12
2.5	Section 5.1.1 Token Inclusion Values	12
2.6	Section 5.4.7 SecureConversationToken Assertion	12
2.7	Section 6.1 [Algorithm Suite] Property	12
2.8	Section 6.4 [Signature Protection] Property.....	13
2.9	Section 6.7 [Security Header Layout] Property.....	13
2.10	Section 7.1 AlgorithmSuite Assertion.....	13
2.11	Section 7.5 AsymmetricBinding Assertion	14
2.12	Section 10.1 Trust13 Assertion	14
3	Normative Errors.....	15
3.1	Section 7.1 AlgorithmSuite Assertion.....	15
4	References.....	16
Appendix A.	Acknowledgements	17

1 Issues Addressed

2 The following issues related to WS-SecurityPolicy 1.2 as recorded in the [WS-SX Issues] have been
3 addressed in this document.

Issue	Description
ER001	Inconsistent IncludeToken URI between spec and schema xsd file
ER002	Editorial comments on SP
ER004	Wrong Security Context Token assertion in example
ER007	Minor editorial addition to <ContentEncryptedElements> Assertion
ER009	Policy Assertion Parameters and alternatives
ER010	Typo in the Security Header Layout section
ER011	Modification request for issue PR014
ER006	Presence of wsu:Timestamp when [Timestamp] is false
ER014	Review normative RFC 2119 language in WS-SecurityPolicy
i165	SP errata
i170	Update XML Signature references to refer to XML Signature, Second Edition, update c14n reference in ws-trust
i171	Incorrect URI provided for Canonical XML 1.0 when defining C14n abbreviation

4

2 Typographical/Editorial Errors

2.1 Normative language capitalization changes

The following changes do not affect the normative meaning of the text, they are only to properly capitalize 2119 terms. The changes listed below document the changes as they appear in the text. There were many instances of the terms OPTIONAL and REQUIRED in the schema exemplar descriptions that appeared un-capitalized that are not captured below but that have also been addressed. All other 2119 terms that remain un-capitalized are used in their English sense.

Line 121

Extensibility points in the exemplar MAY NOT be described in the corresponding text

Line 130

WS-SecurityPolicy SHOULD be applicable to any version of SOAP

Line 321

Assertions MAY be used to further qualify a specific aspect of another assertion. For example, an assertion describing the set of algorithms to use MAY qualify the specific behavior of a security binding

Line 338

Any REQUIRED message elements (e.g. timestamps) in the wsse:Security header

Line 347

Note that a service MAY choose to reject messages despite them conforming to its policy, for example because a client certificate has been revoked. Note also that a service MAY choose to accept messages that do not conform to its policy.

Line 365

This section defines properties that are referenced later in this document describing the RECOMMENDED or REQUIRED attachment points for various assertions.

Line 489

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as separate references in a signature when message security is used

Line 571

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as separate references

Line 597

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as separate references

47 Line 628
48 Multiple instances of this element MAY appear within this assertion and SHOULD be treated as a
49 combined XPath expression
50
51 Line 658
52 Any token assertion MAY also carry an OPTIONAL sp:IncludeToken attribute
53
54 Line 659
55 This attribute indicates whether the token SHOULD be included
56
57 Line 664 (in table)
58 an external reference to the token SHOULD be used.
59 Subsequent related messages sent between the recipient and the initiator MAY refer to
60
61 Line 673
62 A token assertion MAY carry a sp:IncludeToken attribute that requires that the token be included in the
63 message
64
65 Line 684
66 then references to that token are REQUIRED to contain all the specified reference types.
67
68 Line 691
69 Any token assertion MAY also carry an OPTIONAL sp:Issuer element
70
71 Line 696
72 Any token assertion MAY also carry an OPTIONAL sp:IssuerName element.
73
74 Line 703
75 While both sp:Issuer and sp:IssuerName elements are OPTIONAL they are also mutually exclusive
76
77 Line 706
78 Any token assertion MAY also carry an OPTIONAL wst:Claims element
79
80 Line 710
81 This element indicates the REQUIRED claims that the security token MUST contain in order to satisfy the
82 requirements of the token assertion.
83
84 Line 713
85 Individual token assertions MAY further limit what claims MAY be specified for that specific token
86 assertion.
87
88 Line 716

89 As long as the union of all tokens in the received message contains the REQUIRED set of claims from
90 REQUIRED token issuers the message is valid according to the receiver's policy.
91
92 Line 736
93 This boolean property specifies whether derived keys SHOULD be used as defined in WS-
94 SecureConversation
95
96 Line 900
97 Note: The IssuedToken MAY or MAY NOT be associated with key material and such key material MAY
98 be symmetric or asymmetric.
99
100 Line 902
101 Services MAY also include information in the sp:RequestSecurityTokenTemplate element
102
103 Line 1180
104 then either the sp:SecureConversationToken or the sp:IssuedToken assertion SHOULD be used instead
105
106 Line 1187
107 Because this token is issued by the target service and MAY NOT have a separate port
108
109 Line 1379
110 the sp:IssuedToken assertion SHOULD be used instead
111
112 Line 1451
113 the sp:IssuedToken assertion SHOULD be used instead
114
115 Line 1597
116 This property specifies the algorithm suite REQUIRED for performing cryptographic operations with
117 symmetric or asymmetric key based security tokens.
118
119 Line 1635
120 This property indicates the order in which integrity and confidentiality are applied to the message, in
121 cases where both integrity and confidentiality are REQUIRED
122
123 Line 1639
124 This boolean property specifies whether the signature MUST be encrypted.
125
126 Line 1641
127 The primary signature element is NOT REQUIRED to be encrypted if the value is 'true'
128
129 Line 1646
130 This boolean property specifies whether signatures MUST cover the token used to generate that
131 signature.

132
133 Line 1650
134 It is RECOMMENDED that assertions that define values for this property apply to [Endpoint Policy
135 Subject].
136
137 Line 1653
138 This boolean property specifies whether signature digests over the SOAP body and SOAP headers
139 MUST only cover the entire body and entire header elements.
140
141 Line 1661
142 It is RECOMMENDED that assertions that define values for this property apply to [Endpoint Policy
143 Subject].
144
145 Line 1674
146 then it SHOULD appear before the ds:Signature and xenc:ReferenceList elements
147
148 Line 1700
149 then it SHOULD appear before the ds:Signature and xenc:ReferenceList elements
150
151 Line 1719
152 However, the xenc:ReferenceList is NOT REQUIRED to appear before independently encrypted tokens
153 such as the xenc:EncryptedKey token as defined in WSS
154
155 Line 2133
156 Additional tokens MAY be specified to augment the claims
157
158 Line 2134
159 This section defines seven properties related to supporting token requirements which MAY be referenced
160 by a Security Binding
161
162 Line 2145
163 Supporting tokens MAY be specified at a different scope than the binding assertion
164
165 Line 2148
166 the sender SHOULD merge the requirements by including all tokens
167
168 Line 2152
169 all the tokens SHOULD sign and encrypt the various message parts
170
171 Line 2161
172 To illustrate the different ways that supporting tokens MAY be bound to the message
173
174 Line 2165

175 Even before any supporting tokens are added, each binding requires that the message is signed using a
176 token satisfying the REQUIRED usage for that binding
177
178 Line 2171
179 Note: if REQUIRED, the initiator MAY also include in the Security header the token used as the basis for
180 the message signature (Sig1), not shown in the diagram
181
182 Line 2178
183 Supporting tokens are included in the security header and MAY OPTIONALLY include additional
184 message parts to sign and/or encrypt
185
186 Line 2229
187 Signed tokens are included in the “message signature” as defined above and MAY OPTIONALLY include
188 additional message parts to sign and/or encrypt
189
190 Line 2283
191 produced from the message signature and MAY OPTIONALLY include
192
193 Line 2339
194 This assertion MAY OPTIONALLY include additional message parts to sign and/or encrypt
195
196 Line 2345
197 If transport security is used, the token (Tok2) is included in the Security header and the signature (Sig2)
198 SHOULD cover the message timestamp as illustrated below
199
200 Line 2485
201 There are several OPTIONAL aspects to the WSS: SOAP Message Security specification
202
203 Line 2496
204 a token MAY be referenced using different mechanisms
205
206 Line 2551
207 This boolean property specifies whether wsse11:SignatureConfirmation elements SHOULD be used
208
209 Line 2634
210 These assertions relate to interactions with a Security Token Service and MAY augment the behaviors
211 defined by
212
213 Line 2649
214 A challenge issued by the server MAY increase the number of messages exchanged by the client and
215 service
216
217 Line 2656

218 This boolean property indicates whether client entropy is REQUIRED to be used as key material for a
219 requested proof token. A value of 'true' indicates that client entropy is REQUIRED. A value of 'false'
220 indicates that client entropy is NOT REQUIRED

221

222 Line 2661

223 This boolean property indicates whether server entropy is REQUIRED to be used as key material for a
224 requested proof token. A value of 'true' indicates that server entropy is REQUIRED. A value of 'false'
225 indicates that server entropy is NOT REQUIRED

226

227 Line 2881

228 Policy MAY be embedded inside an Issued Token assertion, or acquired out-of-band. There MAY be an
229 explicit trust relationship between the Server and the STS. There MUST be a trust relationship between
230 the Client and the STS.

231

232 Line 2885

233 client-specific parameters that MUST be understood

234

235 Line 2898

236 The Client MAY augment or replace the contents of the RST

237

238 Line 2902

239 The Issued Token Policy Assertion contains elements which MUST be understood by the Client. The
240 assertion contains one element which contains a list of arbitrary elements which SHOULD be sent along
241 to the STS

242

243 Line 2908

244 All items are OPTIONAL , since the Server and STS MAY already have a pre-arranged relationship

245

246 Line 3808

247 A wsse:UsernameToken MAY be encrypted when a transport binding is not being used

248 **2.2 Section 1.5 Normative References**

249 Line 254 changed

250 <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>

251 to

252 <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>

253

254 Inserted after line 254

255 [W3C Recommendation, D. Eastlake et al. XML Signature Syntax and
256 Processing (Second Edition). 10 June 2008.

257 <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/>

258

259 **2.3 Section 2 Security Policy Model**

260 Added after line 288

261 Parameters defined by this specification represent additional information for engaging behaviors that do
262 not need to participate in matching. When multiple security policy assertions of the same type with
263 parameters present occur in the same policy alternative the parameters should be treated as a union.
264 Note that a service may choose to accept messages that do not match its policy.

265 **2.4 Section 4.2.3 ContentEncryptedElements Assertion**

266 Added after line 593

267 If no attribute is provided, then XPath 1.0 is assumed.

268 **2.5 Section 5.1.1 Token Inclusion Values**

269 The schema had token inclusion values defined that did not match the values defined in the specification.
270 The following schema fragment was corrected.

271 Original, incorrect, schema fragment

```
272 <xs:simpleType name="IncludeTokenType">  
273 <xs:restriction base="xs:anyURI" >  
274 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
275 trust/200702/ws-securitypolicy/IncludeToken/Never" />  
276 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
277 trust/200702/ws-securitypolicy/IncludeToken/Once" />  
278 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
279 trust/200702/ws-securitypolicy/IncludeToken/AlwaysToRecipient" />  
280 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
281 trust/200702/ws-securitypolicy/IncludeToken/AlwaysToInitiator" />  
282 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
283 trust/200702/ws-securitypolicy/IncludeToken/Always" />  
284 </xs:restriction>  
285 </xs:simpleType>
```

286 Updated, correct, schema fragment

```
287 <xs:simpleType name="IncludeTokenType">  
288 <xs:restriction base="xs:anyURI" >  
289 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
290 securitypolicy/200702/IncludeToken/Never" />  
291 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
292 securitypolicy/200702/IncludeToken/Once" />  
293 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
294 securitypolicy/200702/IncludeToken/AlwaysToRecipient" />  
295 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
296 securitypolicy/200702/IncludeToken/AlwaysToInitiator" />  
297 <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-  
298 securitypolicy/200702/IncludeToken/Always" />  
299 </xs:restriction>  
300 </xs:simpleType>
```

301 **2.6 Section 5.4.7 SecureConversationToken Assertion**

302 Line 1282 changed

303 <sp:SC10SecurityContextToken />

304 to

305 <sp:SC13SecurityContextToken />

306 **2.7 Section 6.1 [Algorithm Suite] Property**

307 Line 1622 Table entry changed

308 C14n <http://www.w3.org/2001/xml-c14n#>
to
C14N <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>
309
310 Line 1622 Table entry inserted
C14N11 <http://www.w3.org/2006/12/xml-c14n11>
311
312 Line 1622 Table entry changed
ExcC14n <http://www.w3.org/2001/10/xml-exc-c14n#>
313 to
ExcC14N <http://www.w3.org/2001/10/xml-exc-c14n#>
314
315 Line 1627 Table entry changed
[C14n Algorithm] ExcC14n
316 to
[C14n Algorithm] ExcC14N
317

318 **2.8 Section 6.4 [Signature Protection] Property**

319 Lines 1640-1642 changed
320 The primary signature element is not required to be encrypted if the value is 'true' when there is nothing
321 else in the message that is encrypted.
322 to
323 The primary signature element is not required to be encrypted if the value is 'true' when there is nothing in
324 the message that is covered by this signature that is encrypted.

325 **2.9 Section 6.7 [Security Header Layout] Property**

326 Line 1665 table contents changed
327 wsse:Timestamp
328 to
329 wsu:Timestamp

330 **2.10 Section 7.1 AlgorithmSuite Assertion**

331 Inserted after line 1750
332 `<sp:InclusiveC14N11 ... /> ?`
333
334 Line 1819 changed
335 ExcC14N
336 To
337 ExcC14N
338

339 **2.11 Section 7.5 AsymmetricBinding Assertion**

340 Line 2097 changed

341 The specified token populates the [Recipient Signature Token] property and is used for the message
342 signature from Recipient to recipient.

343 to

344 The specified token populates the [Recipient Signature Token] property and is used for the message
345 signature from recipient to the initiator.

346

347 Lines 2103 changed

348 The specified token populates the [Recipient Encryption Token] property and is used for the message
349 encryption from recipient to Recipient.

350 to

351 The specified token populates the [Recipient Encryption Token] property and is used for the message
352 encryption from initiator to recipient.

353 **2.12 Section 10.1 Trust13 Assertion**

354 Line 2720 changed

355 sp:Trust10

356 to

357 sp:Trust13

358 **3 Normative Errors**

359 **3.1 Section 7.1 AlgorithmSuite Assertion**

360 Inserted after line 1819

361 /sp:AlgorithmSuite/wsp:Policy/sp:InclusiveC14N11

362

363 This OPTIONAL element is a policy assertion that indicates that the [C14N] property of an
364 algorithm suite is set to 'C14N11'. Note: as indicated in Section 6.1 the default value of the
365 [C14N] property is 'ExC14N'.

366

367

368

369 **4 References**

- 370 [WS-SX Issues] WS-SX TC Issues List
371 <http://docs.oasis-open.org/ws-sx/issues/Issues.xml>
372 [WS-SecurityPolicy] OASIS Standard, "WS-SecurityPolicy 1.2", July 2007
373 <http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702>

374 **Appendix A. Acknowledgements**

375 The following individuals have participated in the creation of this specification and are gratefully
376 acknowledged.

377
378 TC Members during the development of this specification:
379 Don Adams, Tibco Software Inc.
380 Jan Alexander, Microsoft Corporation
381 Steve Anderson, BMC Software
382 Donal Arundel, IONA Technologies
383 Howard Bae, Oracle Corporation
384 Abbie Barbir, Nortel Networks Limited
385 Charlton Barreto, Adobe Systems
386 Mighael Botha, Software AG, Inc.
387 Toufic Boubez, Layer 7 Technologies Inc.
388 Norman Brickman, Mitre Corporation
389 Melissa Brumfield, Booz Allen Hamilton
390 Lloyd Burch, Novell
391 Scott Cantor, Internet2
392 Greg Carpenter, Microsoft Corporation
393 Steve Carter, Novell
394 Symon Chang, BEA Systems, Inc.
395 Ching-Yun (C.Y.) Chao, IBM
396 Martin Chapman, Oracle Corporation
397 Kate Cherry, Lockheed Martin
398 Henry (Hyenvui) Chung, IBM
399 Luc Clement, Systinet Corp.
400 Paul Cotton, Microsoft Corporation
401 Glen Daniels, Sonic Software Corp.
402 Peter Davis, Neustar, Inc.
403 Martijn de Boer, SAP AG
404 Werner Dittmann, Siemens AG
405 Abdeslem DJAOUI, CCLRC-Rutherford Appleton Laboratory
406 Fred Dushin, IONA Technologies
407 Petr Dvorak, Systinet Corp.
408 Colleen Evans, Microsoft Corporation
409 Ruchith Fernando, WSO2
410 Mark Fussell, Microsoft Corporation
411 Vijay Gajjala, Microsoft Corporation
412 Marc Goodner, Microsoft Corporation
413 Hans Granqvist, VeriSign

414 Martin Gudgin, Microsoft Corporation
415 Tony Gullotta, SOA Software Inc.
416 Jiandong Guo, Sun Microsystems
417 Phillip Hallam-Baker, VeriSign
418 Patrick Harding, Ping Identity Corporation
419 Heather Hinton, IBM
420 Frederick Hirsch, Nokia Corporation
421 Jeff Hodges, Neustar, Inc.
422 Will Hopkins, BEA Systems, Inc.
423 Alex Hristov, Otecia Incorporated
424 John Hughes, PA Consulting
425 Diane Jordan, IBM
426 Venugopal K, Sun Microsystems
427 Chris Kaler, Microsoft Corporation
428 Dana Kaufman, Forum Systems, Inc.
429 Paul Knight, Nortel Networks Limited
430 Ramanathan Krishnamurthy, IONA Technologies
431 Christopher Kurt, Microsoft Corporation
432 Kelvin Lawrence, IBM
433 Hubert Le Van Gong, Sun Microsystems
434 Jong Lee, BEA Systems, Inc.
435 Rich Levinson, Oracle Corporation
436 Tommy Lindberg, Dajeil Ltd.
437 Mark Little, JBoss Inc.
438 Hal Lockhart, BEA Systems, Inc.
439 Mike Lyons, Layer 7 Technologies Inc.
440 Eve Maler, Sun Microsystems
441 Ashok Malhotra, Oracle Corporation
442 Anand Mani, CrimsonLogic Pte Ltd
443 Jonathan Marsh, Microsoft Corporation
444 Robin Martherus, Oracle Corporation
445 Miko Matsumura, Infravio, Inc.
446 Gary McAfee, IBM
447 Michael McIntosh, IBM
448 John Merrells, Sxip Networks SRL
449 Jeff Mischkinisky, Oracle Corporation
450 Prateek Mishra, Oracle Corporation
451 Bob Morgan, Internet2
452 Vamsi Motukuru, Oracle Corporation
453 Raajmohan Na, EDS
454 Anthony Nadalin, IBM
455 Andrew Nash, Reactivity, Inc.

456 Eric Newcomer, IONA Technologies
457 Duane Nickull, Adobe Systems
458 Toshihiro Nishimura, Fujitsu Limited
459 Rob Philpott, RSA Security
460 Denis Pilipchuk, BEA Systems, Inc.
461 Darren Platt, Ping Identity Corporation
462 Martin Raepple, SAP AG
463 Nick Ragouzis, Enosis Group LLC
464 Prakash Reddy, CA
465 Alain Regnier, Ricoh Company, Ltd.
466 Irving Reid, Hewlett-Packard
467 Bruce Rich, IBM
468 Tom Rutt, Fujitsu Limited
469 Maneesh Sahu, Actional Corporation
470 Frank Siebenlist, Argonne National Laboratory
471 Joe Smith, Apani Networks
472 Davanum Srinivas, WSO2
473 Yakov Sverdlov, CA
474 Gene Thurston, AmberPoint
475 Victor Valle, IBM
476 Asir Vedamuthu, Microsoft Corporation
477 Greg Whitehead, Hewlett-Packard
478 Ron Williams, IBM
479 Corinna Witt, BEA Systems, Inc.
480 Kyle Young, Microsoft Corporation