



# Web Services Security: UsernameToken Profile 1.0

## Errata 1.0

### Committee Draft 200401, October 2006

**Document identifier:**

{WSS: SOAP Message Security }-{UsernameToken Profile}-{1.0} (Word) (PDF)

**Document Location:**

<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0-errata-004>

**Errata Location:**

<http://www.oasis-open.org/committees/wss>

**Editors:**

Anthony	Nadalin	IBM
Phil	Griffin	Individual
Chris	Kaler	Microsoft
Phillip	Hallam-Baker	VeriSign
Ronald	Monzillo	Sun

**Contributors:**

Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Lab
Merlin	Hughes	Baltimore Technologies
Irving	Reid	Baltimore Technologies
Peter	Dapkus	BEA
Hal	Lockhart	BEA
Symon	Chang	CommerceOne
Srinivas	Davanum	Computer Associates
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
Paula	Austel	IBM
Bob	Blakley	IBM
Joel	Farrell	IBM
Satoshi	Hada	IBM
Maryann	Hondo	IBM
Michael	McIntosh	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	Konersmann	Microsoft
Chris	Kurt	Microsoft
Brian	LaMacchia	Microsoft
Paul	Leach	Microsoft
John	Manferdelli	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
Steve	Anderson	OpenNetwork (Sec)
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
Blake	Dournaee	Sarvega
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
John	Weiland	US Navy
Phillip	Hallam-Baker	VeriSign
Mark	Hays	Verisign
Hemma	Prafullchandra	VeriSign

15

16 **Abstract:**

17 This document contains a list of errata against WSS Username Token Profile 1.0 that  
 18 have been approved by the WSS Technical Committee.

19 **Status:**

20 This version of the errata is a working draft of the committee. As such, it may change  
 21 prior to incorporation into a future OASIS Standard. Please send comments to the  
 22 editors. If you are on the wss@lists.oasis-open.org list for committee members, send  
 23 comments there. If you are not on that list, subscribe to the wss-comment@lists.oasis-  
 24 open.org list and send comments there. To subscribe, send an email message to wss-  
 25 comment-request@lists.oasis-open.org with the word "subscribe" as the body of the  
 26 message. For patent disclosure information that may be essential to the implementation  
 27 of this specification, and any offers of licensing terms, refer to the Intellectual Property  
 28 Rights section of the OASIS Web Services Security Technical Committee (WSS TC) web  
 29 page at <http://www.oasis-open.org/committees/wss/ipr.php>. General OASIS IPR  
 30 information can be found at <http://www.oasis-open.org/who/intellectualproperty.shtml>.

---

31

## 32 Table of Contents

33	1	Issues Addressed .....	4	
34	2	Typographical Errors.....	4	
35	3	Normative Errors.....	5	
36	3.1	Section 2.2 Namespaces .....	5	
37	3.2	Section 3.1 Usernames and Passwords .....	5	
38	3.3	Section 3.2 Token Reference.....	5	
39	3.4	Section 3.4 Key Derivation (new).....	<u>Error! Bookmark not defined.</u>	Deleted: 6
40	3.5	Section 4 Security Considerations .....	<u>6</u>	Deleted: 7
41	4	Non-Normative Errors .....	<u>7</u>	Deleted: 8
42	5	Clarifications .....	<u>8</u>	Deleted: 9
43		Appendix A: Revision History .....	<u>9</u>	Deleted: 10
44		Appendix B: Notices .....	<u>10</u>	Deleted: 11

45

---

## 46 1 Issues Addressed

47 The following issues have been addressed in this document:

48

ISSUE	DESCRIPTION
259	Editorial comments on Username Token profile - post v1 review period.
461	Remove Key Derivation Section

---

## 49 2 Typographical Errors

50

51 None

---

## 3 Normative Errors

52

### 3.1 Section 2.2 Namespaces

53

54

Add the following after line 81

55

URI fragments defined in WSS: Username Token Profile 1.0 are relative to a base URI of

56

`http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-`

57

`token-profile-1.0`

58

### 3.2 Section 3.1 Usernames and Passwords

59

Delete the following line (89):

60

Passwords of type `wsse:PasswordText` and `wsse:PasswordDigest` are not limited to

61

and replace it with:

62

Passwords of type `PasswordText` and `PasswordDigest` are not limited to

63

64

Delete the following lines (91-93):

65

Having a type of `wsse:PasswordText`, `wsse:PasswordDigest` merely implies that the information held in the password is "in the clear"...

66

and replace it with:

67

68

Having a type of `PasswordText` merely implies that the information held in the password is "in the clear" ...

69

70

71

Delete the following line (98):

72

Passwords of type `wsse:PasswordText` and `wsse:PasswordDigest` are defined as being

73

and replace it with:

74

Passwords of type `PasswordDigest` are defined as being

75

76

Delete the following line (101-102):

77

the digest offers no real additional security over use of `wsse:PasswordText` and

78

`wsse:PasswordDigest`.

79

and replace it with:

80

the digest offers no real additional security over use of `PasswordText`.

81

82

Delete the following line (132):

83

Note that `wsse:PasswordDigest` can only be used if the plain text password (or password

84

and replace it with:

85

86

Note that `PasswordDigest` can only be used if the plain text password (or password

87

88

Delete the following line(235):

89

"ValueType attribute is not required. If specified, the value of `<wsse:UsernameToken>`

90

MUST"

91

and replace it with:

92

"ValueType attribute is not required. If specified, the value of `#UsernameToken` MUST"

93

### 3.3 Section 3.2 Token Reference

94

Delete the following line(235):

95

`ValueType` attribute is not required. If specified, the value of `<wsse:UsernameToken>`

96

MUST

97

and replace it with:

98            ValueType attribute is not required. If specified, the value of #UsernameToken MUST  
99  
100            .

### 101    **3.4 Section 4 Security Considerations**

102            Add after line 282:

103            The security of keys derived from passwords is limited by the attacks available against  
104            passwords themselves, such as guessing and brute force. Because of the limited size of  
105            password that human beings can remember and limited number of octet values  
106            represented by keys that can easily be typed, a typical password represents the  
107            equivalent of an entropy source of a maximum of only about 50 bits. For this reason a  
108            maximum key size of only 160 bits is supported. Longer keys would simply increase  
109            processing without adding to security.

110            The key derivation algorithm specified here is based on one described in RFC 2898. It is  
111            referred to in that document as PBKDF1. It is used instead of PBKDF2, because it is  
112            simpler and keys longer than 160 bits are not required as discussed previously.

113            The purpose of the salt is to prevent the bulk pre-computation of key values to be tested  
114            against distinct passwords. The Salt value is defined so that MAC and encryption keys  
115            are guaranteed to have distinct values even when derived from the same password. This  
116            prevents certain cryptanalytic attacks.

117            The iteration count is intended to increase the work factor of a guessing or brute force  
118            attack, at a minor cost to normal key derivation. An iteration count of at least 1000 (the  
119            default) SHOULD always be used.

---

120 **4 Non-Normative Errors**

121 None

122  
123  
124

---

## 5 Clarifications

The following table lists the full URI for each URI fragment referred to in the specification.

URI Fragment	Full URI
#PasswordDigest	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordDigest">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordDigest</a>
#PasswordText	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText</a>
#UsernameToken	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#UsernameToken">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#UsernameToken</a>

125



126

---

## Appendix A: Revision History

Rev	Date	What
1	06/25/04	First Draft of Errata
2	07/06/04	Updated per comments on list

127

128 This section is non-normative.

---

## Appendix B: Notices

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

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

142 Copyright © OASIS Open 2002-2004. *All Rights Reserved.*

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

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

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

159

160 This section is non-normative.