Project	IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>
Title	Identifying the correct TEK in the TEK State Machine
Date Submitted	2005-10-06
Source(s)	David Johnston Voice: 502 264 3855 Intel Corporation Fax: Hillsboro, OR mailto:dj.johnston@ieee.org USA
Re:	Reply comment to 8001 of the 802.16e recirculation ballot
Abstract	A proposal to disambiguate the key that is being referred to in the TEK state machine
Purpose	To correct errors in the TEK state machine.
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Identifying the Correct TEK in the TEK state machines

David Johnston
Intel Corporation(optional)

Background

The text of the TEK state machine is unclear about what key is being referred to in the key update. The insertion of the work 'newer' in states 8-B and 8-E, along with a change to the diagram clear this up.

This change was proposed for cor1 by Piter-Paul Giesberts. However it did not get properly considered by the group. This document merely recreates that proposal as an edit to 16e. My analysis and that of others I have consulted identify that this proposal is correct ad the error is real.

Proposal

[Change text of 8-B and 8-E of 7.5.2.1 as indicated]

7.2.5.1 Actions

8-B   Op Wait (Key Reply) → Operational

   a) Clear Key Request retry timer
   b) Process contents of Key Reply message and incorporate new keying material into key database
   c) Set the TEK refresh timer to go off "TEK Grace Time" seconds prior to the <u>newer</u> key's scheduled expiration
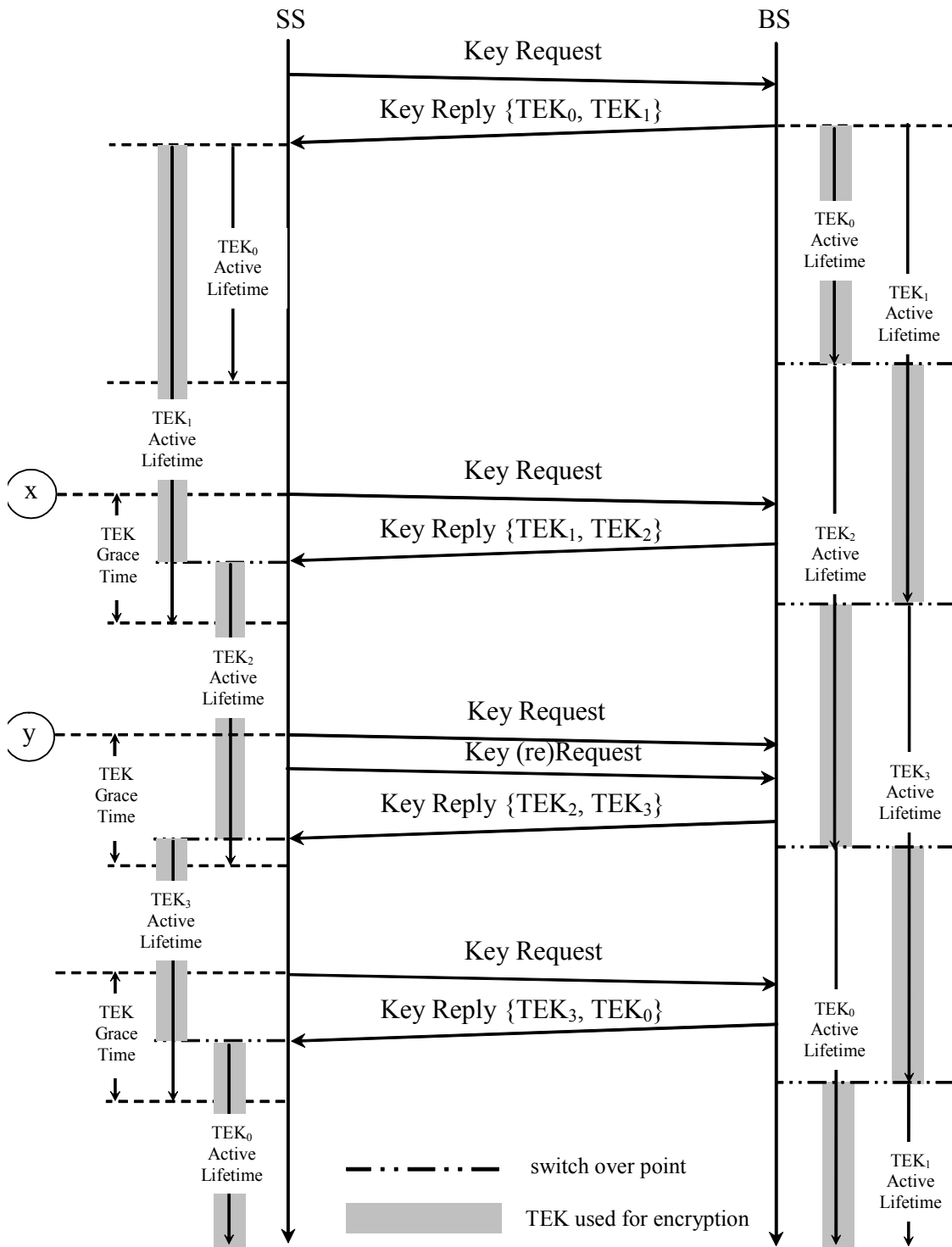
8-E   Rekey Wait (Key Reply) → Operational

   a) Clear Key Request retry timer
   b) Process contents of Key Reply message and incorporate new keying material into key database
   c) Set the TEK refresh timer to go off "TEK Grace Time" seconds prior to the <u>newer</u> key's scheduled expiration

[Replace Figure 134 TEK Management in BS and SS on page 293 with:]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

SS   BS

Key Request

Key Reply {TEK_0, TEK_1}

TEK_0
Active
Lifetime

TEK_0
Active
Lifetime

TEK_1
Active
Lifetime

TEK_1
Active
Lifetime

Key Request

x

TEK
Grace
Time

Key Reply {TEK_1, TEK_2}

TEK_2
Active
Lifetime

TEK_2
Active
Lifetime

Key Request

y

TEK
Grace
Time

Key (re)Request

Key Reply {TEK_2, TEK_3}

TEK_3
Active
Lifetime

TEK_3
Active
Lifetime

Key Request

TEK
Grace
Time

Key Reply {TEK_3, TEK_0}

TEK_0
Active
Lifetime

TEK_0
Active
Lifetime

— · · — · · —   switch over point

TEK_1
Active
Lifetime

TEK used for encryption

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65