Reply Contribution for #115, #331, #332, #333, and #334


Title: Reply Contribution for #115, #331, #332, #333, and #334

Data Submitted: 2006-09-21

Source(s):
Seokheon Cho, Voice: +82-42-860-5524
Jaeseon Cha, Fax: +82-42-861-1966
Chulsik Yoon, chosh@etri.re.kr

Thomas Hallin, Motorola
Mark Cudak, Postdata
Yerang Hur, NextWave
Lei Wang

161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea

Re: IEEE Std 802.16e-2005

Abstract: The contents of the PKM-related parameters in the REG-REQ/RSP messages

Purpose: Adoption of proposed changes into IEEE Std 802.16e-2005

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://iee802.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:chiar@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://iee802.org/16/ipr/patents/notice>.
Reply Contribution for #115, #331, #332, #333, and #334

Seokheon Cho, Jaeseon Cha, and Chulsik Yoon
ETRI

Thomas Hallin and Mark Cudak
Motorola

Yerang Hur
Postdata

Lei Wang
NextWave

Introduction

There are commentaries about security-related parameters in REG-REQ/RSP messages. The those commentaries’ CR numbers in the IEEE maintenance TG are #115, #331, #332, #333, and #334.

The solutions provided by those commentaries are conflict with each other; the solution of #115 is different from the solution of #331, #332, #333, and #334.

Hence, it is necessary to clarify this problem.
Proposed changes

[Change section 6.3.2.3.23: as follows]

6.3.2.3.23 SS basic capability request (SBC-REQ) message

<< Change following parts >>
<< from >>

PKM flow control (see 11.7.8.6)
Authorization policy support (see 11.8.4.2)
Maximum number of supported security association (see 11.7.8.8)

<< to >>

Security Negotiation Parameters (see 11.8.4)

[Change section 6.3.2.3.24: as follows]

6.3.2.3.24 SS basic capability response (SBC-RSP) message

<< Change following parts >>
<< from >>

PKM flow control (see 11.8.4)
Authorization policy support (see 11.8.5)
Maximum number of supported security association (see 11.8.6)

<< to >>

Security Negotiation Parameters (see 11.8.4)
11.7.8 SS Capabilities encodings

Delete 11.7.8.3 MAC CRC support.

Change 11.7.8.6 to 11.8.4 and change its scope to SBC-REQ SBC-RSP.

Change 11.7.8.7 to 11.8.5, change its scope to SBC-REQ SBC-RSP and change the first paragraph as indicated:

This field indicates authorization policy that both SS and BS need to negotiate and synchronize. A bit value of 0 indicates “not supported” while 1 indicates “supported.” If this field is omitted, then both SS and BS shall use the IEEE 802.16 security, constituting X.509 digital certificates and the RSA public-key encryption algorithm, as authorization policy. If this field is present and equal to 0, PKM shall be considered disabled.

Change 11.7.8.8 to 11.8.6 and change its scope to SBC-REQ SBC-RSP.

Delete 11.7.8.6

Delete 11.7.8.7

Delete 11.7.8.8

11.8.4 Security Negotiation Parameters

<table>
<thead>
<tr>
<th>Sub-attribute</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKM Version Support</td>
<td>Version of privacy sublayer supported</td>
</tr>
<tr>
<td>Authorization Policy Support</td>
<td>Authorization policy to support</td>
</tr>
<tr>
<td>Message Authentication Code Mode</td>
<td>Message authentication code to support</td>
</tr>
<tr>
<td>PN Window Size</td>
<td>Size capability of the receiver PN window per SAID</td>
</tr>
<tr>
<td>PKM Flow Control</td>
<td>Maximum number of concurrent PKM transactions</td>
</tr>
<tr>
<td>Maximum Number of Supported Security Associations</td>
<td>Maximum number of supported SA</td>
</tr>
</tbody>
</table>
11.8.4.5 PKM Flow Control

This field specifies the maximum number of concurrent PKM transactions that may be outstanding.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.5</td>
<td>1</td>
<td>0 indicates no limit (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1–255 indicate maximum concurrent transactions</td>
</tr>
</tbody>
</table>

11.8.4.6 Maximum number of supported security associations

This field specifies the maximum number of supported security association of the SS.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.6</td>
<td>1</td>
<td>Maximum number of security association</td>
</tr>
<tr>
<td></td>
<td></td>
<td>supported by the SS (default = 1)</td>
</tr>
</tbody>
</table>

[Change section 12.1.1.1.4.7: as follows]

12.1.1.4.7 REG-REQ

<< Delete text shown in strikethrough >>

—PKM Flow Control (default = no limit)