Comments on Security Sublayer in IEEE 802.16j-06/017r1

IEEE 802.16 Presentation Submission Template (Rev. 8.3)

Document Number:

IEEE C802.16j-06/098

Date Submitted:

2006-09-19

Source:

Yanling Lu	Voice:	+86-10-82882897
Ting Li	Fax:	+86-10-82882383
Shulan Feng	E-mail:	luyanling@hisilicon.com
Hisilicon Technologies		liting@hisilicon.com
Nan Tian Bldg.,No.10,Xinxi.Rd,Hai-Dian District, Beijing ,China		fengsl@hisilicon.com

Venue:

Mont Tremblant, Quebec, Canada

Abstact

This document is a proposal for some comments on Security Sublayer in IEEE 802.16j-06/017r1

Purpose:

This document is provided in response for Call for Contributions IEEE 802.16j Relay Task Group on 2006-09-08

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.

IEEE 802.16 Patent Policy:

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>.

Outline

- The first TOC on “Security Sublayer”
- The second TOC on “Security Sublayer”
- Our opinions

Comments on Security sublayer(1-1)

7 Security Sublayer

Enhanced security features will be required to support multi-hop connections via relay stations.

7.1Architecture

7.1.2 Key management protocol

Insert RS key management at end of this subclause.

7.6 Certificate profile

Insert a subclause at end of 7.6.1.4 to describe RS attributes.

7.6.1.4.4 RS certificate

This section discussed RS attribute to support identity.

Comments on Security sublayer(1-2)

7.10 PKM Version 3

7.10.1Authentication protocol

7.10.1.1 RSA authentication

RSA authentication that support RS

7.10.1.2 EAP authentication

EAP authentication that support RS

7.10.2 Key Usage

This section discusses Keys that used in RS

7.10.2.1 Derivation of Keys used in PKMv3

7.10.2.2 Key derivation function in PKMv3

This section discusses keys and encryption algorithm in RS that will be used authentication when Relay exist.

7.10.3 Message

Insert messages used in the RS in the Key Request, Key Reply and Key Update Command message.

Comments on Security sublayer(2-1)

7 Security Sublayer

Enhanced security features will be required to support multi-hop connections via relay stations.

7.1 Architecture

7.1.2 Key management protocol

Insert RS key management at end of this subclause.

7.2 PKM protocol

7.2.2 PKM Version 2

7.2.2.2 Key derivation

7.2.2.2.2 EAP authentication

Insert EAP authentication that support RS

7.2.3 Security capabilities

Insert some context for BS can select from cryptographic suites of RSs.

Comments on Security sublayer(2-2)

7.3 Key Usage

7.3.3 RS key usage

This section discusses Keys that used in RS

7.5 Cryptographic methods

7.5.4 Derivation of TEKs,KEKs ,and message authentication keys

7.5.4.7 Key derivation function for RS authentication

This section discusses keys and encryption algorithm in RS that will be used authentication when Relay exist.

7.6 Certificate profile

7.6.1 Certificate format

7.6.1.4 tbsCertificate.issuer and tbsCertificate.subject

7.6.1.4.4 RS certificate

This section discussed RS attribute to support RS identity attributes.

Comments on Security sublayer(2-3)

7.8 PKMv2

7.8.2mutual authentication and AK exchange overview

7.8.2.1 BS and SS RSA mutual authentication and AK exchange overview

(Change 7.8.2 in legacy standard tor7.8.2.1)

7.8.2.2 BS,RS and SS RSA mutual authentication and AK exchange overview

This section discusses BS、RS and SS RSA mutual authentication method to support security communication.

7.9 Optional multicast and broadcast rekeying algorithm (MBRA)

7.9.2 Message

Insert messages used in the RS in the Key Request, Key Reply and Key Update Command message.

Our opinions

- The first : modify legacy standard less, new contents are more centralized.
- The second : keep legacy standard structure as possible as it can.
- The first is better.

Thanks!