Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Secure Transport of backbone messages**	
Date Submitted	**2004-05-04**	
Source(s)	Dongkie Lee, DongIl Moon, DongRyul Lee, JongKuk Ahn, Sungho Ha SK Telecom 15F, Seoul Finance Center, 84, Taepyungpro 1 ga, Chung-gu, Seoul, 100-768, Korea	Voice: +82-2-6323-3147 Fax: +82-2-6323-4493 [mailto: {galahad,dimoon,drlee,jgahn,ss23}@sktelecom.com]
Re:	Response to IEEE 802.16-04/19 (Recirculation Ballot #14a Announcement)	
Abstract	To securely transport backbone message, shared secret based encryption for backbone message is proposed.	
Purpose	Discuss and Adopt as the secure backbone message transport mechanism	
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>.	

Secure Transport of backbone messages

Dongkie Lee, Dongll Moon, DongRyul Lee, JongKuk Ahn, Sungho Ha
SK Telecom

1. Problem Statements

Current IEEE 802.16e/D2 does not specify secure backbone transport mechanism. There are some backbone messages which might have sensitive information like security context information, mobility information which requires secure transport mechanism.

2. Overview of Proposed Solutions

When a BS sends backbone message which requires secure transport, it will encrypt the attributes using the method taken from the book *"Network Security" by Kaufman, Perlman and Speciner pages 109-110.* This method is used in encrypting RADIUS User Password and MS-MPPE-Send-Key, MS-MPPE-Rcv-Key.

3. Proposed Changes to IEEE 802.16e

[Add the following text to section D.2.11 after D.2.10 MSS:]

D.2.11 Secure Backbone transport

This field contains encrypted attributes which requires secure transport between backbone nodes. Any backbone message may contain this attribute, but shared secret between backbone nodes shall be provisioned before usage.

Type	Length	Value	Scope
TBD	Variable	Encrypted backbone message attributes except global header	Any backbone message which requires secure transport

Attributes shall be encrypted as follows:

Attributes which requires encryption are first padded at the end with nulls to a multiple of 16 octets. A one-way MD5 hash is calculated over a stream of octets consisting of the shared secret. This value is XORed with the first 16 octet segment of the attributes which is to be encrypted and placed in the first 16 octets of the Value field of the Secure-Backbone-transport Attribute.

If the attributes which is to be encrypted are longer than 16 characters, a second one-way MD5 hash is calculated over a stream of octets consisting of the shared secret followed by the result of the first xor. That hash is XORed with the second 16 octet segment of the password and placed in the second 16 octets of the Value field of the Secure-Backbone-transport Attribute.

If necessary, this operation is repeated, with each xor result being used along with the shared secret to generate the next hash to xor the next segment of the password, to no more than 128 characters.

Call the shared secret S. Break the attributes which is to be encrypted into 16-octet chunks p1, p2, etc. with the last one padded at the end with nulls to a 16-octet boundary. Call the ciphertext blocks c(1), c(2), etc. We'll need intermediate values b1, b2, etc.

b1 = MD5(S) c(1) = p1 xor b1
b2 = MD5(S + c(1)) c(2) = p2 xor b2
. .
. .
. .
bi = MD5(S + c(i-1)) c(i) = pi xor bi

The Value field will contain c(1)+c(2)+...+c(i) where + denotes concatenation. On receipt, the process is reversed to yield the original attributes.