Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Secure Transport of backbone messages**
Date Submitted	**2004-07-07**
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:	Recirculation Ballot #14b Announcement
Abstract	To securely transport backbone message, reference to shared secret based encryption for backbone message text 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, DongIl Moon, DongRyul Lee, JongKuk Ahn, Sungho Ha
SK Telecom
Junhyuk Song, Samsung

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 may encrypt the attributes using the method taken from the RFC 2548, RFC2865. This method is used in encrypting RADIUS User Password(RFC 2865) and MS-MPPE-Send-Key, MS-MPPE-Rcv-Key(RFC 2548).

Some text from RFC 2548 is as follows:

2.4.2. MS-MPPE-Send-Key

Description

The MS-MPPE-Send-Key Attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). As the name implies, this key is intended for encrypting packets sent from the NAS to the remote host. This Attribute is only included in Access-Accept packets.

A summary of the MS-MPPE-Send-Key Attribute format is given below. The fields are transmitted left to right.

```
 0               1               2               3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Vendor-Type | Vendor-Length |           Salt
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type

16 for MS-MPPE-Send-Key.

Vendor-Length

> 4

Salt

The Salt field is two octets in length and is used to ensure the uniqueness of the keys used to encrypt each of the encrypted attributes occurring in a given Access-Accept packet. The most significant bit (leftmost) of the Salt field MUST be set (1). The contents of each Salt field in a given Access-Accept packet MUST be unique.

String

The plaintext String field consists of three logical sub-fields: the Key-Length and Key sub-fields (both of which are required), and the optional Padding sub-field. The Key-Length sub-field is one octet in length and contains the length of the unencrypted Key sub-field. The Key sub-field contains the actual encryption key.

If the combined length (in octets) of the unencrypted Key-Length and Key sub-fields is not an even multiple of 16, then the Padding sub-field MUST be present. If it is present, the length of the Padding sub-field is variable, between 1 and 15 octets. The String field MUST be encrypted as follows, prior to transmission:

Construct a plaintext version of the String field by concatenating the Key-Length and Key sub-fields. If necessary, pad the resulting string until its length (in octets) is an even multiple of 16. It is recommended that zero octets (0x00) be used for padding. Call this plaintext P.

Call the shared secret S, the pseudo-random 128-bit Request Authenticator (from the corresponding Access-Request packet) R, and the contents of the Salt field A. Break P into 16 octet chunks p(1), p(2)...p(i), where i = len(P)/16. Call the ciphertext blocks c(1), c(2)...c(i) and the final ciphertext C.

Intermediate values b(1), b(2)...c(i) are required. Encryption is performed in the following manner ('+' indicates concatenation):

b(1) = MD5(S + R + A) c(1) = p(1) xor b(1) C = c(1)

b(2) = MD5(S + c(1)) c(2) = p(2) xor b(2) C = C + c(2)

. .

. .

b(i) = MD5(S + c(i-1)) c(i) = p(i) xor b(i) C = C + c(i)

The resulting encrypted String field will contain c(1)+c(2)+...+c(i). On receipt, the process is reversed to yield the plaintext String.

3. Proposed Changes to IEEE 802.16e

3.1 Option 1 - Detailed Text on Backbone message security

[Add the following text before section D.3 and change D.3 and so on to D.4:]

D.3 Inter-base station message Attributes Format
D.3.1 Secure Backbone transport

This field may 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 according to MS-MPPE-Send-Key section of RFC 2548.

Vendor-Type and Vendor-Length in RFC 2548 are not used. The pseudo-random 128-bit Request Authenticator (from the corresponding Access-Request packet) R of RFC 2548 is replaced with 128-bit concatenation of Sender BS-ID(48-bit), Target BS-ID(48-bit), Time Stamp(32-bit). Constructing a plaintext version of the String field is done by concatenating the attributes which requires secure transport and if necessary, padding the resulting string until its length (in octets) is an even multiple of 16.

3.2 Option 2 – Short Text on Backbone message security

[Change D.1 as following:]

D.2 Inter-base station message formats

The message formats described in this section may be used for communication with peer BS or with an ASA server through the backbone. When a BS sends backbone messages that contain confidential information, such as key materials, it may be encrypted and message authenticated.

D.2.1 Global Message Header

The global message header is a collection of fields required ay all inter-base station messages. The header is defined in Table D4.