Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>
Title	**MS Identity Privacy in 802.16m**
Date Submitted	**2009-1-5**
Source(s)	Haihong Zheng, Shashikant Maheshwari, Yousuf Saifullah **NSN** Jan Suumaki **Nokia**
	Haihong.Zheng@nsn.com jan.suumaki@nokia.com
Re:	TGm SDD: 10.6.2.1 AMS Privacy
Abstract	Propose temporary station identifier to support MS identity privacy
Purpose	For discussion and adoption in 802.16m SDD
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups.* It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.

MS Identity Privacy in 802.16m

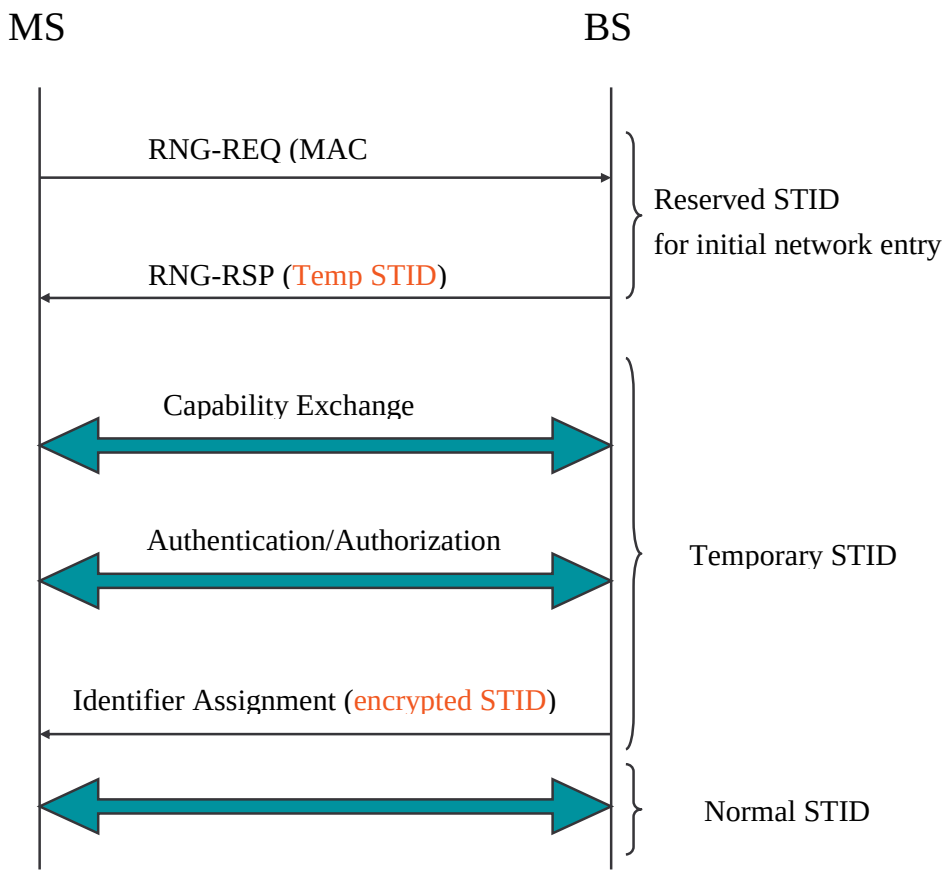
Haihong Zheng, Shashikant Maheshwari, Yousuf Saifullah
Nokia Siemens Networks

Jan Suumaki
Nokia

I. Introduction

In reference system there is no explicit means by which identity of user is protected. During initial ranging and certificate exchange during authorization AMS MAC Address (AMS ID) is transmitted in the clear. Hence, the identity or location information can be easily inferred from fixed AMS MAC address, result of which violates the security aspects of IEEE 802.16m SRD. However, sending MAC address over the air cannot be completely avoided. MAC address is needed for BS to obtain MS related information from other network entities. MAC address is used by ABS to generate various security keys. Certificate which contains MAC address is sent over the air in clear text. How to protect MAC address in the initial ranging and certificate needs more study. However, the mapping between MAC address and Station ID should be solved. This is because by monitoring the ranging procedures, an intruder can obtain the mapping between MAC address and Station ID, based on which perform specific attack to that specific user.

In order to solve the problem above, a Temporary Station Identifier (STID) is assigned during initial ranging process. After being assigned, it is used for the subsequent network entry procedures until the normal STID is allocated. Normal STID is assigned during/after authentication process, and the assignment message shall be encrypted. The temporary STID is then released and normal STID is used for all the remaining transactions. The detailed procedure is illustrated in the following figure.



II. Text Proposal

========== *Start of Proposed Text* ==========

10.6.2.1: AMS Privacy

~~In reference system there is no explicit means by which identity of user is protected. During initial ranging and certificate exchange during authorization AMS MAC Address (AMS ID) is transmitted in the clear. Hence, the identity or location information can be easily inferred from fixed AMS MAC address, result of which violates the security aspects of IEEE 802.16m SRD. Detailed method for providing AMS ID privacy is FFS.~~

In order to protect the mapping between the STID and the AMS MAC Address, two types of station identifiers are assigned to an AMS during network entry - temporary STID (TSTID) and (normal) STID.A TSTID is assigned during initial ranging process, and is used until the STID is allocated. The STID is assigned during the authentication process, and the assignment message is encrypted. The TSTID is released after STID is assigned. The STID is used for all the remaining transactions.

========== *End of Proposed Text* ==========