Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	SA-TEK Corrections	
Date Submitted	**2005-09-07**	
Source(s)	Simon Mizikovsky, Robert Rance Lucent Technologies	Voice: 973-386-6348, 978-952-1513 Fax: 973-386-4555 mailto:smizikovsky@lucent.com, rrance@lucent.com
Re:	Call for contribution and comments.	
Abstract	A change in the labeling of the MS-originated nonce in the SA-TEK 3-way handshake causes several problems.	
Purpose	Adoption	
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>.	

SA-TEK Corrections

Simon Mizikovsky, Robert Rance
Lucent Technologies

Problem Definition

Background

As part of the SA-TEK 3-way handshake in 802.16e/D10 draft, the MS creates a freshly-generated number called MS_Random. The BS also generates a random number called BS_Random. Inclusion of these numbers in the handshake guarantees freshness of the messages.

MS_Random and BS_Random also occur in the PKMv2 RSA messages, and MS_Random also occurs in the PKMv2 Authenticated EAP Start messages.

First Problem

In 802.16e/D8, 6.3.2.3.9.18 "SA-TEK-Request message", Table 37h "SA-TEK-Request message attributes": NonceMS is defined as "A 64-bit number chosen by the MS (once per protocol run). This can be a counter or a random number."

In 802.16e/D9, 6.3.2.3.9.19 "PKMv2 SA-TEK-Request message", Table 37h "PKMv2 SA-TEK-Request message attributes": NonceMS was relabeled as MS_Random, and redefined as "A 64-bit number chosen by the MS freshly for every new handshake." This change was carried over into 802.16e/D10, 6.3.2.3.9.19 "PKMv2 SA-TEK-Request message", Table 37i "PKMv2 SA-TEK-Request message attributes”.

While this redefinition does not preclude using a counter, its label and redefinition steers one away from such use. For some mobile manufacturers, using a counter here can provide better security since the mobile may not have a good entropy source and thus be unable to generate certifiably good random numbers. Conversely, implementing a sufficiently and provably entropic random number generator in the mobile may add cost.

Use of a counter rather than a random number for the MS-generated nonce preserves security because no other (adversarial) party can produce a PKMv2 SA-TEK-Request message with the same count. Receipt and authentication of this message is necessary for the BS to return with a PKMv2 SA-TEK-Response message.

Note: Because an extra precaution has been taken of authenticating the PKMv2 SA-TEK-Challenge message with the HMAC/CMAC Digest, the BS_Random number could also be generated by a counter. However, random numbers are in general much easier to generate in the BS for at least two reasons: Many MS calls are being processed, each of which can contribute entropy; and the cost of a random number generator can be amortized over many MSs. Thus we do not recommend replacing the designation and definition of BS_Random.

Second Problem

In 802.16e/D10, 6.3.2.3.9.11 "PKMv2 RSA-Request message", Table 37a "PKMv2 RSA-Request attributes": MS_Random is defined as “A 64-bit random number generated in the MS”.

So, in 802.16e/D10, MS_Random is used in two different contexts, one as a freshly chosen number for the

SA-TEK handshake, and the other as a random number for RSA-based authorization. Using the same label for different random numbers can be confusing to the developer.

Third Problem

In 802.16e/D10, the notations BS_Random and MS_Random are used in both the PKMv2 RSA messages, 6.3.2.3.9.11 through 6.3.2.3.9.14, and in the PKMv2 SA_TEK messages, 6.3.2.3.9.18 through 6.3.2.3.9.20. Additionally, MS_Random is used in 6.3.2.3.9.28 “PKMv2 Authenticated EAP Start”. There is a risk that a developer would interpret the D10 specification such that the same random numbers could be used for all of these applications, and that would be insecure.

That such an erroneous interpretation could occur can be seen in the wording that was used in 802.16e/D8, 6.3.2.3.9.18 "SA-TEK-Request message", Table 37h "SA-TEK-Request message attributes": "A 64-bit number chosen by the MS (once per protocol run). …”. The notion of a protocol run (now discarded), could be interpreted as a combined PKMv2 RSA and PKMv2 SA_TEK protocol run.

Proposed Text Changes

Changes to handle first and second problems

The text changes below will solve the first and second problems above.

[Modify the corresponding sections as follows:]

[Change the first attribute row in 802.16e/D10, 6.3.2.3.9.19 "PKMv2 SA-TEK-Request message", Table 37i "PKMv2 SA-TEK-Request message attributes” as:]

~~MS_Random | A 64-bit number chosen by the MS freshly for every new handshake.[a]~~

NonceMS | A 64-bit number chosen by the MS freshly for every new handshake. This can be a counter or a random number.[a]

[Change the first attribute row in 802.16e/D10, 6.3.2.3.9.20 "PKMv2 SA-TEK-Response message", Table 37j "PKMv2 SA-TEK-Response message attributes” as:]

~~MS_Random~~ | The number received from the MS

NonceMS | The number received from the MS

Changes to handle third problem

[Add the following text (or equivalent) at the end of 802.16e/D10, 6.3.2.3.9.11 “PKMv2 RSA-Request message” (or other appropriate place):]

Whenever a random or freshly generated number is required as part of a message it cannot be reused from another, identically-labeled instance of it from a different message. For example, MS_Random in this message must be different from MS_Random in the PKMv2 Authenticated EAP Start message.