Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	PMK Refresh
Date Submitted	**2005-07-18**
Source(s)	Simon Mizikovsky, Robert Rance, Peretz Feder Lucent Technologies Voice: 973-386-6348 Fax: 973-386-4555 mailto:smizikovsky@lucent.com
Re:	Call for contribution and comments.
Abstract	A method for refreshing the PMK (Pairwise Master Key) without re-contacting the AAA-Server.
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>.

PMK Refreshing

Simon Mizikovsky, Robert Rance, Peretz Feder
Lucent Technologies

Problem Definition

Background

A Master Session Key (MSK) is generated from the Root Key MK. This key is derived as recommended in the IETF RFC 3748 “Extensible Authentication Protocol” section 7.10, and is known only to Authentication Server (AAA Server) and the supplicant (MSS)[1] .

The Authentication Server populates the MSK in the corresponding Authenticator using RADIUS or DIAMETER. This is done during the key distribution phase.

From the MSK, a PMK (Pairwise Master Key) is derived. Generation of the PMK marks the successful completion of Credential Verification and User Authentication

Finally from the PMK, an Authorization Key (AK) is generated for a MSS and the BS by both the MSS and the Authenticator. Additional keys are derived from AK as documented in the IEEE 802.16e draft.

Description of the Problem

A security association established between the MSS and access network, as expressed by the PMK, may be retained for a long time if the mobile stays within the boundary of the current Security Domain. Therefore, the Access Key (AK) generated for specific Base Station (BS) and defined as a static function of the PMK, Base Station ID, and MSS ID, will be set to the same value for as long as the PMK is the same.

The current 802.16e standard defines only one way of changing the PMK – and that is to invoke the full three-party EAP authentication procedure. This includes accessing the AAA Server in the subscriber’s home network, which is a lengthy process.

It is desirable to periodically refresh the PMK (and thus the AK) to maintain required security, but to avoid accessing the AAA server in the home network. This refresh is needed for several reasons, such as:

Because the PMK lifetime is close to expiration

To limit the opportunity of passive and active attacks by the adversaries on a static values of PMK and AK

To compensate for a difference in trust for various Base Stations in the serving network served by the same Authenticator. In this case, the less trusted BS will receive the AK based on a newly refreshed PMK, and prior values of security keys would not assist in crypt-analyzing new keys.

To allow quick renewal of the PMK when both it and the AK are erased due to an 802.16e-specified security operation

To allow renewal of PMK, AK and KEK independent of MSK refresh requirements that could be independently used to derive MN-HA and other related mobility keys (i.e. MN-FA).

Remedy

In 802.16e, we are suggesting that the initial value of PMK be generated in the Authenticator and the MSS as a one-way application-specific hash of the MSK, specifically, PMK = H(MSK || “PMK”) where H is a hash

[1] It has been recommended by IETF that the term AAA-Key is misleading, and the key resulting from the EAP process is the MSK itself.

function SHA-1 as in FIPS-180-2, the || denotes concatenation, and "…" denotes a string.

We further suggest to add to 802.16g the PMK Refresh procedure as described in the proposed text. It will allow on demand refreshment of the PMK without re-contacting the AAA Server to update the MSK. Generation of the PMK marks the successful completion of Credential verification and User Authentication i.e. Phase 2. The key management between the authenticator and the supplicant is used to bind the PMK to the supplicant and the authenticator, thereby confirming that both possess the PMK.

Proposed Text Changes

[Modify the corresponding sections as follows: Insert new subsection 14.5.5.2.1]

14.5.5.2.1 PMK Refreshing

After initial establishment, the PMK may be periodically refreshed by executing the PMK Refresh procedure between the Authenticator and the MSS. The procedure is shown on Figure 1 below and is defined as follows:

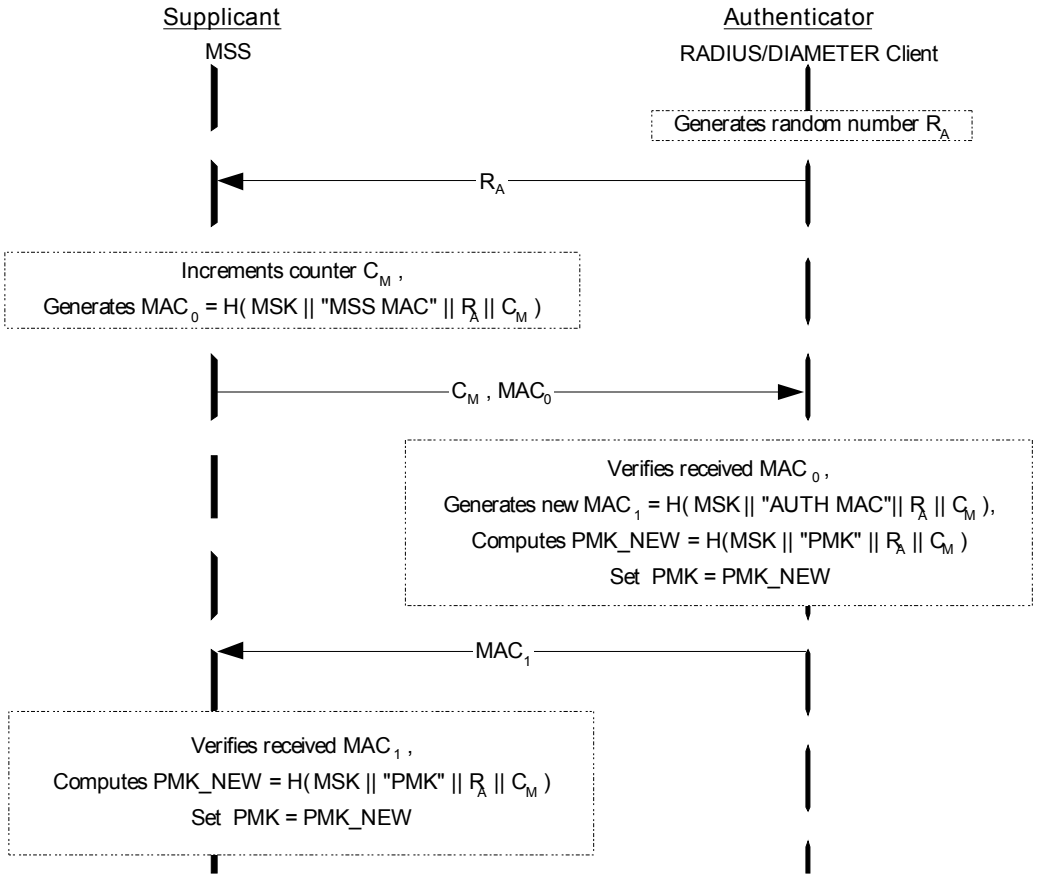

Figure 1 – PMK Refresh Protocol

The initial PMK generated at the completion of the EAP Access Authentication is defined as SHA(MSK || "PMK").

In the figure above, H( ) denotes HMAC-SHA 160( ), the symbol || means concatenation, and value "…" denotes the string.

The protocol is initiated by the Serving Network. In the first message, the network sends the 64-bit random challenge R_A to the MSS.

The mobile maintains a local 32-bit access counter, which it increments every time the PMK needs to be refreshed. The counter is reset when the initial PMK is generated at the end of the EAP exchange. The MSS increments the counter C_M, and computes the MAC (Message Authentication Code) of the returned transaction as
$MAC_0 = H(MSK || \text{“MSS MAC”} || R_A || C_M)$.

The mobile sends the response message to the network containing the C_M and MAC_0.

The serving network validates the MAC_0, and then computes its own

$MAC_1 = H(MSK || \text{“AUTH MAC”} || R_A || C_M)$.

The network also computes the new value of the PMK:

$PMK\_NEW = H(MSK || \text{“PMK”} || R_A || C_M)$.

In the returned message the network sends the MAC_1 to the MSS for validation.

The MSS validates the MAC_1 as an indication of successful completion of the mutually authenticated protocol, and computes the new PMK as shown above.

If the protocol is received uncorrupted, both sides know with cryptographic certainty that they have generated a matching secret key PMK_NEW. At this point the current active value of the PMK is set to the computed PMK_NEW. Otherwise, if the protocol is corrupted in either direction, the corresponding party will detect this and abort the transaction, leaving the current value of the PMK intact.