Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Mobility sensitive master key derivation and fast re-authentication for 802.16m**
Date Submitted	**2007-02-23**
Source(s)	Ronald Mao, Madjid Nakhjiri Huawei Technologies Co.,Ltd. 10180 Telesis Ct, Suite 365 San Diego, CA 92121 Voice: 858-882-0335 Fax: 858-882-0350 mailto: rmao@huawei.com, mnakhjiri@huawei.com Xiaolu Dong RITT Voice: +86-10-62302438 Fax: +86-10-68034801 mailto: dongxiaolu@mail.ritt.com.cn
Re:	Respond to 80216m-07_004, Call for Contributions on Requirements for P802.16m -Advanced Air Interface
Abstract	802.16e uses EAP-based authentication and key management for providing link level security keys. EAP keying framework does not provide support for low latency handover security establishments and re-authentication. IETF HOKEY working group is now designing a new key management framework with the first hand goal of mobility support as well as prevention of domino effect resulting from compromise of authenticator/base station complex in mind. This document puts forward a requirement to use the HOKEY key hierarchy instead of the EAP key hierarchy for 802.16m.
Purpose	Propose the requirements to Section 6.5 (security) of the 802.16m requirement document: IEEE 802.16m-07/002, for an optional use of HOKEY key hierarchy as an alternative to EAP key hierarchy when deriving PMK at each authenticator before calculating AK and KEKs.
Notice	
Release	
Patent Policy and Procedures	

Mobility and delay sensitive master key derivation for 802.16m

Ronald Mao, Madjid Nakhjiri
Huawei Technologies
and Xiaolu Dong
RITT

Proposed text to section 6.5 of IEEE 802.16m-07/002

802.16m key derivation hierarchy should include a new optional branch allowing the use of a HOKEY based PMK derivation (using per authentication master keys, such as MDMSK) in addition to the use of an EAP based PMK derivation (using MSK). This will provide great flexibility and less complex WiMAX architecture design, while at the same time providing great deal of backward compatibility with 802.16e MS and BS, since no portion of the 802.16e key hierarchy below the PMK needs to be changed.

Background: Problems with EAP support for mobility

IEEE 802.16e uses Extensible Authentication Protocol (EAP) as an optional authentication procedure. Given the flexibility of EAP towards a) use of cryptographic algorithm-de-jour for authentication, b) ability to interact with AAA infrastructures and backend AAA servers, it is very likely that EAP will become the de-facto authentication method for 802.16e access control. Furthermore, ability of the new EAP authentication methods in generating session-based master session keys (MSK and EMSK) adds to attraction of use of EAP as key management framework. 802.16e specification describes how the per-base station authorization keys (AK) can be derived from the EAP MSK and the so called pair-wise master key (PMK).

However, due to its roots in providing point to point access service for fixed clients, EAP lacks the inherent ability to deal with end client mobility or the need for end client to quickly extend its session before the initially authorized session expires. As the protocol was designed for fixed operation, the MSK after derivation at the AAA server is transferred to the authenticator at the edge of the network. The authenticator then using the MSK can establish a security association with the client and communicate security (TEK in case of 802.16e). Support of mobile clients has become tricky: if the client moves from one point of attachment to the next, it needs to establish a new security association to the new point of attachment. To avoid the latency associated with the security association re-establishment, many network architectures have chosen to simply transfer the link security keys from one base station to the next. This can create the so called domino effect, i.e. if the security of one base station is compromised, it can lead to the compromise of the security of all the following base stations.

To avoid the problem described above, a so called principle of least privilege [AAAKEY] is applied where each entity gets the minimum amount of security information to continue its operation. This means the authenticator architecture in WiMAX specification has been split into a key distributor (typically in the ASN_GW) and key receiver (typically in the base station), where the former holds MSK and PMK, and calculates the per-base station AK, while keeping MSK and PMK hidden from the base station.

The above solves the base station to base station handover security provisioning to some extent by providing an anchoring mechanism. However, when the end client moves to a base station served by a new authenticator (ASN_GW), the new authenticator does not possess an MSK to perform AK derivations for the new base station. Principle of least privilege prohibits against MSK transfer to the new authenticator. In order to avoid the need for a new EAP exchange (to obtain a new MSK), the WiMAX architecture needs to rely on an anchoring mechanism, where the old authenticator creates the AKs for the new base station. Thus the new base station is said to belong to a mobility domain that is served by the old authenticator. Anchoring can cause its own

problems, aside from possible delays, the AK transfer security may be jeopardize since the old authenticator and new BS would typically belong to different topology.

Another problem associated with use of EAP based MSKs for keying is that in the current state of the art in WiMAX architecture, when a mobile node moves across authenticators served by different access service providers (cross access service provider handovers), the anchoring method can no longer be applied. The mobile node is force to re-authenticate using EAP. EAP authentications, such as EAP-TLS, EAP-TTLS, etc are lengthy procedures comprising of multiple roundtrips taking in order of magnitudes or seconds or more, even though the authentication is performed with the same home CSN and quite possibly the previous authenticated session is still valid. A fast re-authentication mechanism, where the state of previous authentication can be used, can achieve significant reduction in the delay involved with such mobility patterns.

To deal with the problem of handover security, a new working group, called handover keying (HOKEY) is formed in IETF. HOKEY is exploring the use of EAP EMSK for derivation of keys for a variety of use cases, including handovers. Furthermore, HOKEY is specifying a key hierarchy where the EAP MSK or EMSK can be used to directly derive per-authenticator master session keys (can be seen as mobility domain master session keys, MDMSKs). This would mean a new MDMSK would be delivered to each authenticator following an initial EAP authentication or as part of an authenticator handover (proactively or reactively). This way no authenticator anchoring would be required and both mobility performance and security of link layer key management can be improved.

Furthermore, as part of its key hierarchy specification, HOKEY is specifying mechanisms for fast re-authentication, where special re-authentication keys, derived from the EMSK can be used to achieve re-authentication by one or at most two roundtrips.

802.16e backward compatibility concerns

HOKEY working group is taking backward compatibility with EAP very seriously, especially cases where a EAP compliant authenticator needs to work with a HOKEY compliant peer or vice versa. In case of 802.16m, this would for instance mean a HOKEY compliant 802.16m device would need to interoperate with an 802.16e authenticator/BS and vice versa. An 802.16e compliant peer or authenticator would simply use MSK to create the PMK, while an 802.16m compliant peer or authenticator would use MDMSK to create PMK. The HOKEY is considering transport of both MSK and MDMSK to the initial authenticator to address this issue. The functionality of 802.16m base station would not change, since it works off AK, whose derivation is transparent to the way PMK is derived.

References

[AAAKEY], Housley, R. and B. Aboba, "Guidance for AAA Key Management", draft-housley-aaa-key-mgmt-06.txt, Internet draft (work in progress), November 2006.