

802.16e Security Motivations and Needs

IEEE 802.16 Presentation Submission

Document Number:

IEEE C802.16e-04/118

Date Submitted:

2004-05-19

Source:

David Johnston

Intel

2111 NE 25th

Hillsboro, OR 97124

Voice: 503 264 3855

Fax: 503 202 5047

E-mail: dj.johnston@intel.com, david.johnston@ieee.org

Venue:

May 2004 802.16 Interim, Schenzen, China

Base Document:

Purpose:

To illuminate the issues and requirements for 802.16e security Adhoc.

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.

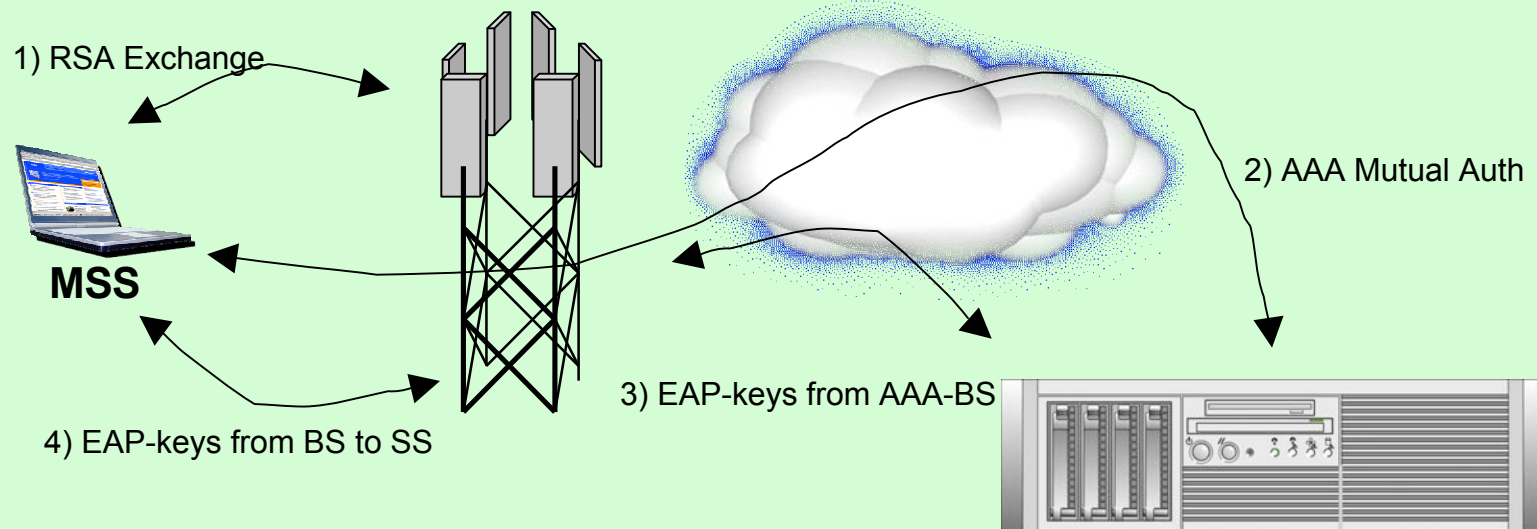
IEEE 802.16 Patent Policy:

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>>.

802.16e Security Adhoc Motivations and Needs

David Johnston, Intel,
dj.johnston@intel.com

Authentication Model



- Two authentications – Cert exchange & EAP
 - Two sets of keying material
- Ultimately leads to keys to protect link traffic

• Are we agreed on this model??

Why?

- Device authentication
 - Verify that the device is OK
 - WiMax Certified, employer issued, Operator issued
- User authentication
 - Verify that the user is OK
 - Is a user that has paid the bill
 - Is a legitimate user – employee, guest, etc.
- Confidentiality
 - Protect privacy, defend against theft of service, forgery & replay
- System Stability
 - Protect the provision of service from DoS
- System Performance
 - Fast Handover
- Dual Authentication
 - Verify that connection is from a legitimate user, using legitimate equipment
 - Very flexible model
 - Model varies depending on who is CA

What it is not

- End to End security
 - We are securing the link and the data on the link
 - We are not protecting data once it has left the BS into the network
- An attempt to do 'pure' security
 - Would not involve EAP or X.509
 - We are following industry norms
- Secure from government snooping
 - Would need 512 bit keys, layered crypto algorithms, non-FIPS, very costly.

Basic Approach

- I think that we all are following certain ways of doing things..
 - RSA key agreement/mutual authentication
 - EAP key agreement/mutual authentication
 - Derive keying for key transfer
 - Timely key updates
 - Out of band security protocol
- Is this true?

What if we don't amend PKMv2?

- Reluctance on operator deployments
 - Want secure basis for billing
 - Want seamless handover for voice
- Reluctance for users to deploy
 - Theft of service
 - Privacy violations
- Reluctance for campus deployments
 - Same as for WEP

Current Security Problems

- Certificate exchange
 - Not mutual
 - Uses X.509 (ugh!)
- Fast Handover
 - No support
- Key Hierarchy
 - No support for EAP keys
- EAP Messages not protected
- Key Exchange
 - Forgery attacks, MITM attacks
 - No EAP key exchange

Current Security Problems

- Authorization state
 - No AAID to distinguish authentication instances
- DES Insecure
 - Poor IV construction
- No management message protection allows DoS and EAP weakness
 - De-register messages, PKM messages etc.
- Inter BS, Inter operation handover performance
 - Tradeoff between security and on-air bandwidth consumption

Current Draft Text Problems

- Protocol Version Number
 - Not tied to any text
 - .16e is current amending the .16d PKMv1 text!
- Authorization Policy Negotiation
 - Is being confused with PKM version negotiation
 - {EAP, mutual auth, good keying} == PKMv2
 - {!EAP, one way auth, bad keying} == PKMv1
- DES Endianess Ambiguity
- No version 2 state machines
- No vectors – Impossible to be interoperable

Technical Approaches

- DJ (Intel) PKMv2
 - Restricted crypto primitives (AES, RSA)
 - Nice for HW
 - Complete Key hierarchy
 - Group key separation
 - EAP-key & PAK binding
 - Fast Handover
 - Pre-Auth (BSID addressed PKM messages)
 - Authorized Association state
 - Mutual Certs with key liveness checking
 - EAP 4 way handshake

Technical Approaches

- Jeff (Streetwaves)
 - PKM-EAP messages
 - EAP messages 4 way handshake
 - Fast Handover
 - PMK Caching

Technical Approaches

- ? (Samsung)
 - Secured PKM packets
 - Map BS EAP to PKM-req and SS EAP to PKM-rsp
 - Individual Negotiation for RSA and EAP exchanges
 - Auth Policy Support
 - MBS service crypto (above ARQ)
 - Crypto Synchronized MAC for Mgmt frames

Technical Approaches

- Donnie Lee (SK Telecom)
 - Map BS EAP to PKM-req and SS EAP to PKM-rsp
 - EAP-Success ACK with PKM message
 - Auth Policy Support
 - Between old and new protocols

New Work

- Define AES based KDFs
- Define MBS <-> GAK link
- GAK Key Transfer
 - Decision : Unicast, Multicast or Both?
- Fast Handover
 - Decision : PMK Caching or Pre Auth or Transfer of derived keys?
- Draw State Machines
- Test Vectors

Proposal Merging

SK Telecom

Samsung

Intel

Streetwaves

New Work

EAP tx/rx separation	EAP tx/rx separation	Key Hierarchy	PMK Caching	PKM Version Link
EAP-ACK	Mgmt Frame Protection EAP Protection	Mutual Cert Exchange AK Xfer		GAK Xfer
	MBS Link	4 Way Handshake	4 way handshake	KDFs
		auth associaion AAID		State Machines
		Pre Auth Packets		Test Vectors
		AES/RSA Algorithms		

EAP tx/rx separation	Key Hierarchy		PKM Version Link
EAP-ACK?	Mutual Cert Exchange AK Xfer	4 Way Handshake	GAK Xfer
Mgmt Frame Protection EAP Protection	auth associaion AAID	Pre-Auth or PMK caching	KDFs
MBS Link	AES/RSA Algorithms		State Machines
			Test Vectors