暗号プロトコル評価対象の概要

独立行政法人　情報通信研究機構

1. プロトコル名：PKM (Privacy and Key Management Protocol)

2. 関連する標準：IEEE Std 802.16e-2005

http://standards.ieee.org/getieee802/download/802.16e-2005.pdf

3. 暗号プロトコル仕様

PKM (Privacy and Key Management protocol) について解説する。

3.1. 暗号プロトコルの概要と目的

WiMAX 通信において、端末(SS/MS)と基地局(BS)との鍵共有を行い、暗号化通信により通信内容を保護する。

シーケンス図

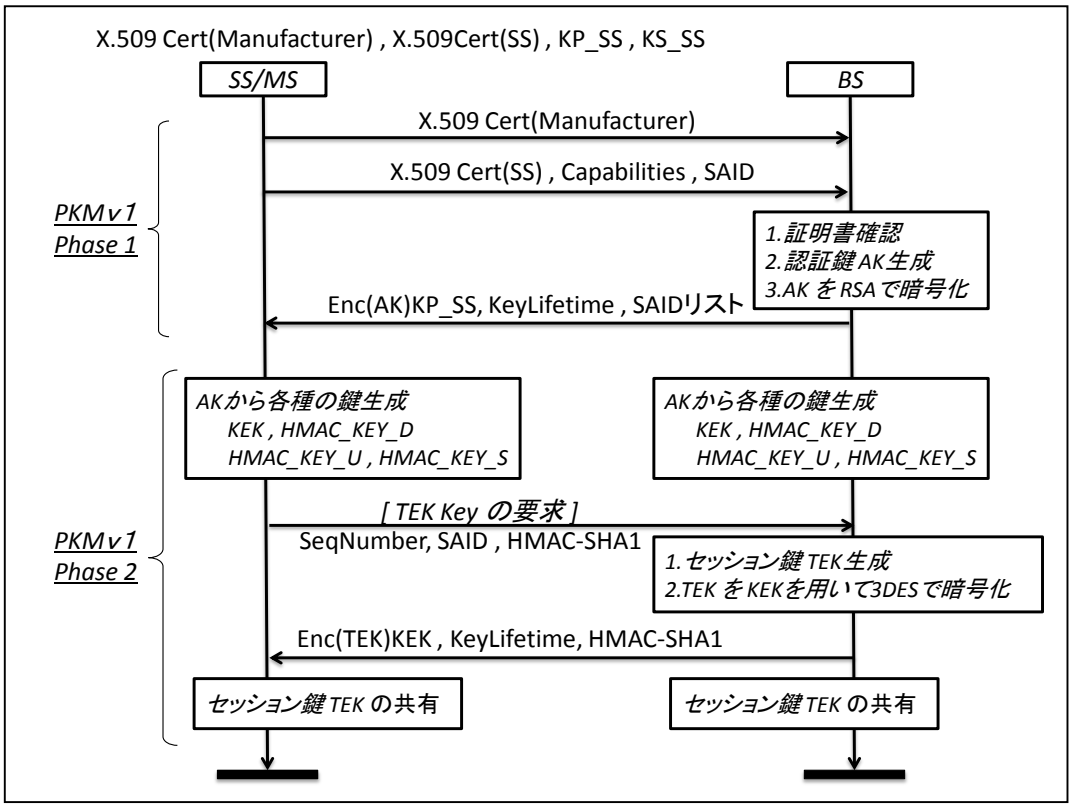

図 1. シーケンス図 (PKMv1 の Phase1 及び Phase2)

PKMv1 では証明書ベースの認証方式と、EAP ベースの認証方式が利用可能であり、証明書ベ

ースの認証方式のサポートが必須となっている。ここでは、証明書ベースの 認証方式について通信シーケンスを記載する。また、上記のシーケンス図では、認証に加えて TEK の共有も同時に行っている。

なお、シーケンス図中の記号は以下の意味で用いられる。

表 1. シーケンス内における記号の意味

記号	意味
BS, SS, SA,	ロール(役割)のラベル
X.509Cert(Manufacturer)	SS の製造メーカ自身のデジタル証明書
X.509Cert(SS)	SS の製造メーカ(又は信頼できる外部機関)が、SS 端末毎に発行するデジタル証明書 (SS 端末の公開鍵 KP_SS や、SS 端末の MAC アドレスが記載)
X.509Cert(BS)	BS に関するデジタル証明書 (PKMv2 で使用)
Security Capability	SS 側でサポートしている暗号アルゴリズムの種類など
SAID	SA の ID
SA	暗号方式や、鍵情報などのセット (Security Associations)
KP_SS, KS_SS	ロール SS の鍵ペア (KP_SS が公開鍵、KS_SS が秘密鍵)
KP_BS, KS_BS	ロール BS の鍵ペア (KP_BS が公開鍵、KS_BS が秘密鍵) (PKMv2 で使用)
AK	認証鍵 (Authorization Key) PKMv1 では、BS で生成される PKMv2 では、PAK を Dot16KDF 関数を用いて導出される。
prePAK	pre-Primary Authorization Key(PKMv2 で使用)
PAK	Primary Authorization Key prePAK を Dot16KDF 関数を用いて導出される。(PKMv2 で使用。)
key lifetime	AK の有効時間
SeqNumber	シーケンスナンバー
SAID リスト	SAID の一覧
TEK	通信を暗号化するためのセッション鍵 (Traffic Encryption Key) AK とは独立に、BS で生成される 64 or 128bit の鍵
KEK	暗号化鍵を暗号化する際の鍵 (Key Encryption Key) AK から生成される 128bit の鍵

4. 評価の環境

4.1. 攻撃者モデル（自然言語による記述）

WiMAX は広域での通信が可能な無線通信方式である。したがって、通信の盗聴や不正なメッセージの送信は容易である。この 2 つに比べるとメッセージの改ざんは比較的難しいが、不可能ではない。

4.2. セキュリティプロパティ（自然言語による記述）

PKMv1 の認証（及び鍵交換）プロトコルでは、基地局（BS）によるクライアント端末（SS）の認証を行う。ここでは、偽端末によるなりすましを防止することが目的である。また、BS と SS の間で認証鍵 AK 及びセッション鍵 TEK の共有を行う。これらの鍵が攻撃者に知られることがあってはならない。

4.3. 暗号プロトコルに関して知られている結果

以下文献のとおり、PKMv1 の評価が行われており、いずれも中間者攻撃が可能という結果を得ている。

・Ahmed M. Taha, Amr T. Abdel-Hamid, and Sofiene Tahar . Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool . 2009 ESRGroups France.
http://eee.guc.edu.eg/Members/TAs/Ahmed%20Taha/Papers/N2S09.pdf

・Kahya Noudjoud, Debbah Adel and Nacira Ghoualmi . WiMAX Security - A Formal Analysis using Scyther tool . ICCTAI'2012 (International Conference on Computational Techniques and Artificial Intelligence) .
http://psrcentre.org/images/extraimages/212083.

・Ender Yuksel . Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis . Kongens Lyngby 2007 IMM-THESIS-2007-16.
http://www2.imm.dtu.dk/~ey///Publications/07Yuk.pdf

・Sridevi and S. Rajaram . Compressed Key Exchange and Key Caching in PKMv2-EAP Mobile WiMAX Authentication . European Journal of Scientific Research ISSN 1450-216X Vol.71 No.3(2012),pp.403-417.
http://www.europeanjournalofscientificresearch.com/ISSUES/EJSR_71_3_09.pdf

・Nirwan Ansari . WiMAX Security：Privacy Key Management

http://www.it.ecei.tohoku.ac.jp/~kato/workshop2007/01.pdf

・Laurent BUTTI . WiMAX: Security Analysis and Experience Return
http://www.first.org/conference/2007/papers/butti-laurent-slides.pdf

・Karen Scarfone,Cyrus Tibbs,Natthew Sexton. Guide to Securing WiMAX Wireless Communications . National Institute of Standards and Technology. Special Publication 800-127 (NIST SP800-127)
http://csrc.nist.gov/publications/nistpubs/800-127/sp800-127.pdf

・Taeshik Shon, Bonhyun Koo, Jong Hyuk Park and Hangbae Chang . Novel Approaches to EnhanceMobileWiMAX Security
http://downloads.hindawi.com/journals/wcn/2010/926275.pdf

・Sen Xu, Chin-Tser Huang, Manton M. Matthews . Modeling and Analysis of IEEE 802.16 PKM Protocols using CasperFDR.
http://www.cse.sc.edu/~huangct/WC086454.pdf

5.備考

本文書は、**総務省「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負　成果報告書」**からの引用である。