PKMv2 の概要

国立研究開発法人 情報通信研究機構

1. 基本情報

- ✧ 名前

  PKM (Privacy and Key Management Protocol Version 2)

- ✧ 機能

  Wimax 通信における端末 (SS/MS) と基地局 (BS) 間の認証・鍵交換プロトコル。

- ✧ 関連する標準

  IEEE Std 802.16e-2005

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

2. プロトコル仕様

PKMv2 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る。本文書では、証明書ベースの認証方式についてシーケンスを図 1 に示す。また、シーケンス図では、認証に加えて鍵 TEK の交換も同時に行っている。なお、シーケンス図中の記号の意味は表 1 に示す。

3. 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。よって、攻撃者として Dolev-Yao モデルを想定する。すなわち、通信の盗聴、改ざん、遮断、再送が可能とする。

4. セキュリティ要件（自然言語による記述）

- ➢ 認証：PKMv2 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。
- ➢ 鍵交換：BS と SS の間で認証鍵 AK 及びセッション鍵 TEK を共有する。これらの鍵が攻撃者に秘匿されている。

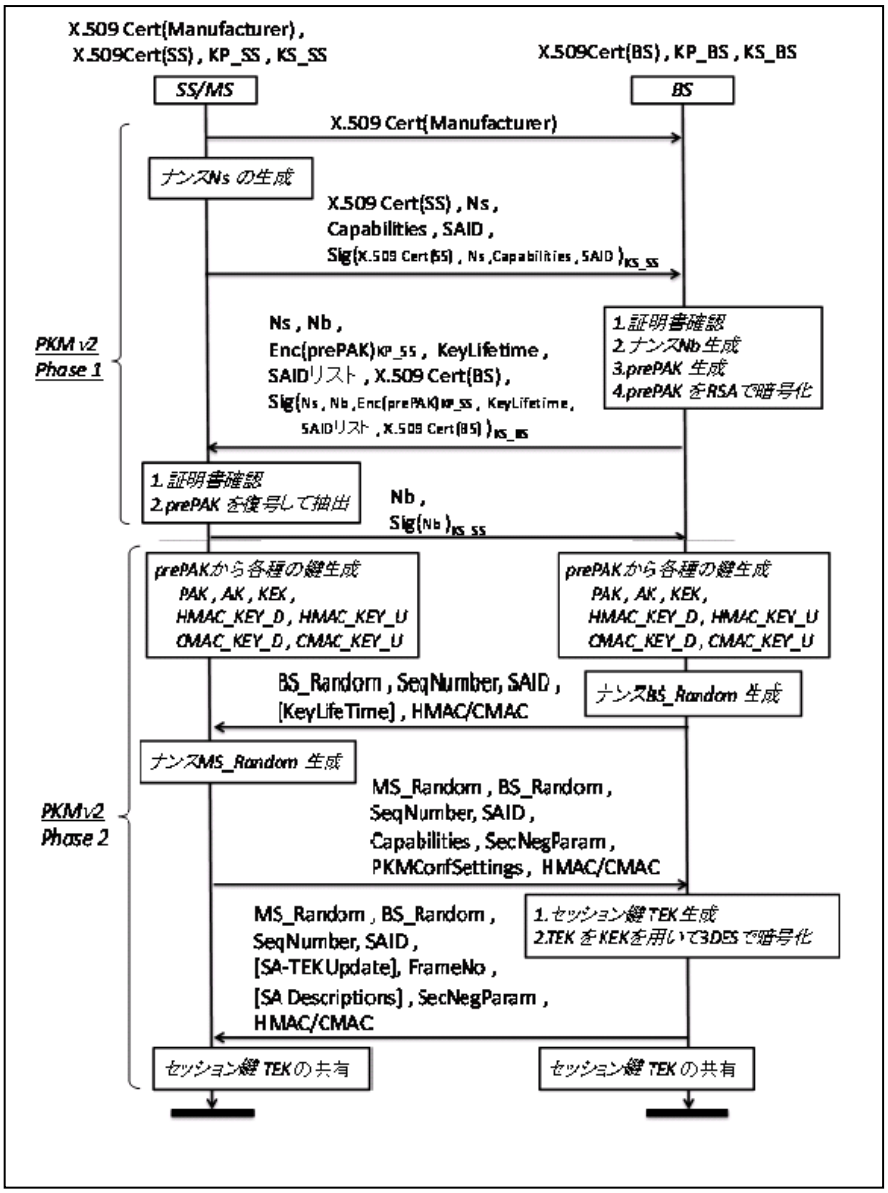

図 1. シーケンス図（PKMv1 の Phase1 及び Phase2）

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

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

PKMv2 について、以下文献のとおり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が得られている。

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

5.2. 形式手法に基づく検証

上述の 2 件が形式手法に基づく検証による評価結果である。

6. 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。