Computer Science and Application 计算机科学与应用, 2013, 3, 293-296
http://dx.doi.org/10.12677/csa.2013.37051 Published Online October 2013 (http://www.hanspub.org/journal/csa.html)

Automatic Root Key Management Based on PKI

Yun Bai, Hui Li, Dongxun Jin

School of Computer Science, Beijing University of Posts and Telecommunications, Beijing
Email: byby_1@126.com, lihuill@bupt.edu.cn, jindongxun0529@gmail.com

Received: Sep. 23rd, 2013; revised: Oct. 20th, 2013; accepted: Oct. 28th, 2013

Abstract: Some of current mobile communication systems represented by 3G systems do not support root key updating, others lack a secure updating method. This paper proposes a root key management scheme which is based on asymmetric encryption and can apply to most of mobile communication systems. This scheme simulates the common using scene of root key in mobile communication systems and protects the security of root key updating by PKI (Public Key Infrastructure). To improve the availability of the system, this scheme gives a modification for root key management. We analyze these improvements' impact on the scheme efficiency taking WPKI for example.

Keywords: Root Key Management; PKI; Digital Certificate; Digital Signature

一种基于 PKI 的根密钥自动管理方案

白　云，李　晖，金东勋

北京邮电大学计算机学院，北京
Email: byby_1@126.com, lihuill@bupt.edu.cn, jindongxun0529@gmail.com

收稿日期：2013 年 9 月 23 日；修回日期：2013 年 10 月 20 日；录用日期：2013 年 10 月 28 日

摘　要：以 3G 系统为代表的移动通信系统中，根密钥的管理存在缺乏更新机制或更新机制不安全的问题。本文提出了一种适用于移动通信系统的基于非对称加密的根密钥管理方案。该方案模拟了移动通信系统中根密钥的一般使用场景，通过使用 PKI (Public Key Infrastructure)技术保证根密钥的安全更新。为了提高可用性，该方案改进了密钥管理流程，本文以 WPKI 为例分析了这些改进对方案效率的影响。

关键词：根密钥管理；PKI；数字证书；数字签名

1. 引言

现代密码体制中，多采用多级密钥机制。这种机制下，下级密钥受上级密钥保护，而根密钥是多级密钥体系的源头，任何下级密钥都要直接或间接的受根密钥保护。因此，根密钥安全是该密钥体系安全的基础和保证。

在很多系统中根密钥的管理以简单易用为主。以 3G 通信系统为例，在 3G 认证与密钥协商协议(AKA)中，密钥体系采用了认证主密钥和通信密钥两层架构，其中认证主密钥 K 为根密钥，通信密钥包括 CK (加密密钥)和 IK (完整性密钥)，他们是 K 的下级密钥，是用户与系统在进行认证期间由 K 通过安全算法派生而来[1]。

在 3G 通信系统中，K 由系统生成，分别存储于用户的 USIM 卡和系统 HLR/AuC 中，不支持更新[2]。随着根密钥使用时间的增长，密钥泄露的可能性增

大。根密钥一旦泄露就只能换卡。这种做法开销很大，而且由于密钥泄露不易检测，还可能造成其他损失，如用户机密信息泄露，用户利益损失等[3,4]。

在对称加密机制下更新根密钥可以使用下述方案：

1) 使用旧根密钥保证新密钥的安全。但若旧密钥已经泄漏，新密钥将很容易被破译。

2) 通过增加密钥层数，即添加上层密钥管理根密钥来支持根密钥的更新。这种方法中，顶层密钥变成了实际的根密钥，依然要面临更新难的问题。

3) 预先在通信两端配置多个根密钥，更新根密钥时换为其它密钥即可。但预先配置的密钥有限，一旦全部用完，还将面临根密钥更新难的问题。而且预先配置的密钥可能一次全部泄漏，因此，这种方法依然有安全隐患[5]。

上述方法均单一的使用对称加密机制管理根密钥。相对于非对称加密机制，这些方案的开销更小，更适用于过去性能较低的终端[3,4]。但现在随着终端性能的提升，在终端上运行非对称算法已成为可能，并出现以 WPKI 为代表的无线安全技术[6]。

2. PKI、WPKI 技术

公开密钥基础设施(PKI)，是一种遵循标准的密钥管理平台，它能够为所有的网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理。目前，PKI 技术已广泛应用于 Internet 安全体系中。各实体通过 PKI 保证各自根密钥的安全。由于 PKI 对终端的存储与计算能力要求较高，为了适应无线通信系统，在 PKI 的基础上衍生出了 WPKI 技术[7]。

WPKI 是一个无线公开密钥体系，是将互联网电子商务中的 PKI 安全机制引入无线网络系统，形成的一套具有严格标准的密钥和证书管理平台体系，并以此为依据管理移动网络环境中的数字证书和所使用的密钥，最终形成一个安全可靠的无线网络环境[8]。

同 PKI 相比，WPKI 简化了证书内容，减少了实体间的通信量[6]。提高了系统效率，但还具有下列问题：

1) 移动终端还是要存储证书并进行非对称计算。这对终端性能是一个考验。

2) 移动终端数过多，证书数量大，导致 CA 压力过大。

3) 通信模式的互通性不强。无线网络与有线网络采取不同的通信模式(WPKI，PKI)，这就在一定程度上影响了二者之间互通的顺畅性[6,7]。

3. 一种根密钥管理方案

针对上述问题，本文提出一种基于 PKI 的根密钥管理方案。该方案可以支持根密钥的更新，并解决了使用 WPKI 管理根密钥所面临的问题。

3.1. 符号说明

为了方便后续讨论，在表 1 中列出了符号以及对应的含义。

3.2. 方案详述

该方案由根密钥管理中心(以下简称 RKMC)、卡管理中心(以下简称 CMC)、认证中心(以下简称 AuC)、密钥加载端(KDE)和移动设备(MS)组成。RKMC 为该方案的核心部分，负责根密钥的管理；CMC、AuC 分别模拟了卡商和系统认证端；KDE 负责在用户卡下发后，为其更新密钥。方案实施可划分为两阶段：1) 离线加载私钥及公钥证书阶段；2) 在线自动下发根密钥阶段。

第一阶段如图 1 所示。首先由 CA 向 RKMC、CMC、AuC 下发数字证书。3 份证书由同一 CA 签发，用于后续的认证。证书部署完成后，由 CMC 在发卡前为每个用户生成公私钥对，公钥发送至 RKMC (图中 1)，私钥写入用户卡内。至此部署阶段已完成。

1) CMC->RKMC: $SigSK_{CMC}||Cert_{CMC}||Receiver||SeqNum||MS1||PK_{MS1}||MS2||PK_{MS2}||\ldots\ldots||MSn||PK_{MSn}$。其中 $SigSK_{CMC}$ 为后续内容的签名。

第二阶段如图 2 所示，RKMC 负责为每个用户生成 RK，并根据需要向用户和 AuC 派发或更新旧 RK。其中，RK 经 AuC 公钥和用户卡公钥加密后分别派发给 AuC (图中 1)和 KDE (图中 2)。KDE 负责向用户下发、更新根密钥。

图中 1、2 均通过文件传输完成。

1) RKMC->AuC: $SigSK_{RKMC}||Cert_{RKMC}||Receiver||SeqNum||MS1||EPK_{AuC}(RK1)||MS2||EPK_{AuC}(RK2)||\ldots\ldots||MSn||EPK_{AuC}(RKn)$。其中，$SigSK_{RKMC}$ 为后续内容的签名。

接收端验证 $SigSK_{RKMC}$ 后，获取 RK: $DecryptSK_{AuC}$

Table 1. Symbols
表 1. 符号说明

符号	含义
RKMC	根密钥管理中心
CMC	卡管理中心
AuC	认证中心
KDE	密钥加载端
CA	证书授权中心
MSn	用户 n 移动终端
$Cert_i$	实体 i 的证书，i 可以是 RKMC、CMC、AuC 或 KDE。
Pk_i	实体 i 的公钥，i 可以是 RKMC、CMC、AuC、KDE 或 MS。
Sk_i	实体 i 的私钥，i 可以是 RKMC、CMC、AuC、KDE 或 MS。
$Sig_{SK}(M)$	使用 SK 对 M 做签名
$E_K(M)$	使用 K 对 M 做对称加密
Receiver	文件接收者
SeqNum	序列号
RK	根密钥

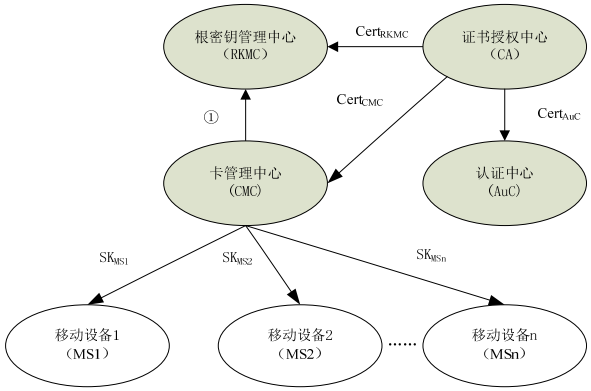

Figure 1. Deployment process
图 1. 部署流程图

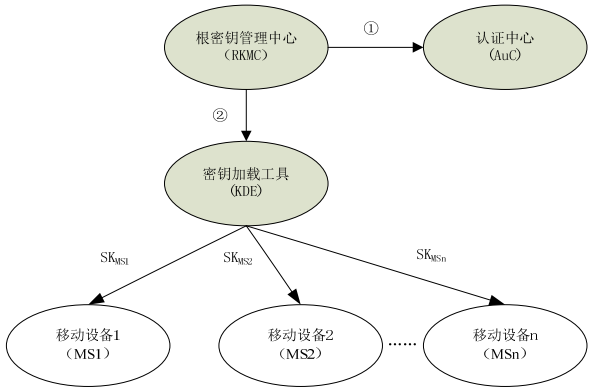

Figure 2. Update root key
图 2. 更新根密钥流程

($EPK_{AuC}(RK)$).

2) RKMC->KDE：$SigSK_{RKMC}||Cert_{RKMC}||Receiver||SeqNum||MS1||EPK_{MS1}(RK1)||MS2||EPK_{MS2}(RK2)||……||MSn||EPK_{MSn}(RKn)$。其中，$SigSK_{RKMC}$ 为后续内容的签名。

接收端验证 $SigSK_{RKMC}$ 后，获取 RK：$DecryptSK_{MS}(EPK_{MS}(RK))$。

至此，MS 与 AuC 分别持有明文 RK，RK 可用于后续的认证过程。

上述讨论详细描述了各模块间的通信过程，为了更好的理解系统的工作过程，下面对系统的细节做一些补充说明：

1) 本方案不讨论 KDE 如何向 MS 下发根密钥，但建议实际系统中 KDE 可以有多个，分别对应不同范围的 MSI，并部署于不同地点。各 MS 需在指定 KDE 处更新根密钥。

2) 本方案中 RKMC、CMC、AuC、KDE 所持证书均为同一 CA 签发。协议中发送信息的一方持有接收方的证书。

4. 方案分析

本方案保证了根密钥更新的安全性，并为提升效率做了一些改进。以下就这 2 方面进行说明。

4.1. 安全性分析

1) 由于方案各部分间均为单向通信，所以协议只需保证接收方对发送方的单向认证即可。信息接受方通过 CA 验证发送方证书的正确性，因此协议支持单向认证。

2) 各协议头部的签名字段保证通信内容的完整性。

3) 数字签名机制保证协议的不可否认性[9]。

4) 序列号防止重放攻击。

5) 通信内容中的敏感信息均使用接收方公钥加密，机密性得以保证。

4.2. 方案特性分析

与 3G 系统的根密钥管理方案不同，本方案支持根密钥更新。本方案使用非对称算法管理根密钥，同对称算法相比效率偏低。但随着用户设备在存储、计

算能力上的提高，非对称算法的开销已渐渐可以接受了。而且同使用对称算法管理根密钥相比，本方案有如下优点：

1) 密钥更新更安全

使用对称算法管理根密钥，无论使用几级密钥，一旦上层密钥泄露，下层密钥的更新都不再安全。而本方案中，只要各模块私钥不泄露，即可保证安全更新。

2) 方便分级管理

由于各模块私钥都存储于本地，不会和其它模块共享，因此安全性不依赖于其它模块。各模块可根据安全需求采取相应的安全管理力度。比如，引入RKMC 后，由 RKMC 管理根密钥。不同于 AuC，RKMC 可以物理隔离，通过离线文件的方式下发根密钥，因而减少了遭受黑客攻击的可能，增加了根密钥的安全性。

3) 减少密钥数

实际系统中 KDE、AuC 数量较多，对称密钥算法将产生大量密钥，不易管理，而使用非对称算法，可减少密钥管理的复杂度。

4) 增加了系统内部的不可否认性

各模块均使用数字证书，保证了系统内部模块间的不可否认性，提升了系统安全性。

本方案解决了使用 WPKI 的根密钥管理方案所面临的问题：

1) MS 只需进行非对称加解密计算，而不必存储证书或进行证书操作。证书相关操作由 KDE 进行。从而提升了终端的效率。

2) 将 MS 的证书简化为公私钥对，并使用 RKMC 管理各 MS 的公钥，有效的减少了证书的数量和 CA 证书管理的复杂度。

3) 本方案在各模块中均使用 PKI 标准的证书(X509)，避免了 WPKI 中无线网和有线网互通性的问题。

表 2 对使用 WPKI 技术的根密钥管理方案和本方案在安全性和性能上做了比较。比较结果显示：本方案在保证根密钥管理安全性的基础上，提升了系统效率。

Table 2. Security and performance contrast
表 2. 安全性、性能对比

	WPKI	RK management based on PKI
服务端对 MS 认证	√	√
完整性	√	√
不可否认性	√	√
机密性	√	√
MS 持有证书	√	×
CA 维护 MS 证书	√	×
MS 非对称运算	√	√
无线网络使用 WPKI	√	×

5. 结束语

本文所提出的根密钥管理方案，通过使用 PKI 技术，解决了以 3G 系统为代表的无线通信系统中根密钥更新困难的问题。经分析，该方案在保证根密钥安全更新的同时，为提升系统效率做了改进。同 WPKI 技术相比，该方案通过引入密钥加载端简化了 MS 证书管理流程，减轻了用户设备负担和 CA 维护证书的数量，从而提高了系统可用性；该方案还有效避免了无线网络与有线网络无法互通的问题。而且随着用户设备能力的提升，该方案的可用性会越来越高。

参考文献 (References)

[1] 3GPP TS 33.102. 3rd Generation partnership project (3GPP); Technical Specification Group (TSG) SA; 3G security; Security threats and requirements. 2011.

[2] H. Ekstrom, A. Furuskar, J. Karlsson and M. Meyer. Technical solutions for the 3G long-term evolution. Communications Magazine, 2006.

[3] C. Zemao, Z. Junge and H. Biyi. Optimizing PKI for 3GPP authentication and key agreement. The 4th International Conference on Multimedia Information Networking and Security (MINES), 2012.

[4] S. Ray, G. P. Biswas. Design of mobile-PKI for using mobile phones in various applications. International Conference on Recent Trends in Information Systems (ReTIS), 2011.

[5] 刘利军, 刘斐, 魏冰. 3G 用户根密钥安全机制研究[R]. 信息通信网络技术委员会年会征文, 2007.

[6] B. Zhang. Research on mobile electronic commerce security technology based on WPKI. Fifth International Conference on Digital Image Processing. International Society for Optics and Photonics, 2013.

[7] P. Tiejun, Z. Leina. New mobile commerce security solution based on WPKI. 2012 International Conference on Communication Systems and Network Technologies (CSNT), 2012.

[8] 耿秀华. 基于证书的信任管理研究[M]. 知识产权出版社, 2011.

[9] J. Katz. Digital Signatures. National Defence Industry Press, 2012.