基于 XKMS 的 PKI 服务的设计与实现

唐韶华　　甘志勇
（华南理工大学计算机科学与工程学院　广州　510640）

摘　要：该文介绍了基于 XKMS 而开发的 PKI 系统，该系统可以提供基于 XKMS 的 PKI 服务。该文分别对该系统的系统设计、开发环境进行了详细描述，并且给出了系统运行实例、测试分析。实测及分析表明，该系统运行效率高，具有跨平台、可移植性好等特性。

关键词：XKMS，PKI，SOAP，Web 服务
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2005)02-0314-03

The Design and Implementation of XKMS-Based PKI Services

Tang Shao-hua　　Gan Zhi-yong
(*School of Computer Science and Engineering, South China University of Technology, Guangzhou* 510640, *China*)

Abstract　A PKI system based on XKMS, which can provide XKMS-based PKI services, is introduced in this paper. This paper also describes the system design, developing environment in more details. The running instances, testing and analysis of this system are also given. By testing and analysis, it indicates that the system has the properties of high efficiency, cross-platform, and good portability.

Key words　XKMS, PKI, SOAP, Web Services

1　引言

近年来，信息安全已经成为极度热门的话题，特别是电子商务及电子政务的兴起使信息安全问题更为突出，传统 PKI（Public Key Infrastructure）技术可以很好地满足当前信息安全的需要。但是由于应用程序必须理解 PKI 架构，而大多数应用程序例如数据库、交易处理软件等不能很好地识别 PKI，这在一定程度上限制了 PKI 的广泛应用。

为解决这些问题，Microsoft，VeriSign，webMethods 三家公司联合制定了 XML（eXtensible Markup Language，可扩展标注语言）密钥管理规范，即 XKMS（XML Key Management Specification）[1]，并提交给 W3C 组织形成一项公开的信息安全标准。XKMS 的研究与实现具有相当重要的意义，它使得开发人员可以透明地看待复杂的、不易理解的传统 PKI，用标准的 XML 工具包——如 XML 签名规范和 XML 加密规范，快速开发出具备所要求功能的应用程序。由于 XML 语言[2]是一种可扩展标记语言，用 XML 表示的信息能够被不同的系统所识别，有利于实现不同平台间的数据共享。因此，XKMS 将进一步推动 PKI 系统在 Internet 上的应用。目前国际上已有众多研究机构对 XKMS 进行了深入研究，国内也有许多研究人员投入到 XKMS 的研究中，例如张剑青等[3]也开发了基于 XML 的 XKeySec 系统。

本文对 XKMS 进行了分析研究，并按照 W3C 组织发布的标准开发设计了 XKMS 的服务器端和客户端软件，其中服务器端软件以 Web Services[4-6]形式予以发布，为客户提供证书注册、证书重发、证书撤销、密钥恢复、证书验证及证书公钥查询等功能，客户端软件用于与服务器端进行通信并完成相应操作。

本文安排如下：第 2 节对 XKMS 作出简单分析和概述，第 3 节给出基于 XKMS 的 PKI 服务的设计与实现方案，第 4 节介绍系统的运行结果、测试分析和性能分析，第 5 节对全文作小结。

2　XKMS 概述

2000 年 11 月 W3C 组织发布了由 Microsoft，VeriSign，webMethods 三家公司共同制定的 XKMS 1.0 草案，这标志着关于 XKMS 的研究初具雏形。2001 年 3 月正式发布了 XKMS 1.0 版，包括 XML 密钥信息服务规范（X-KISS）和 XML 密

2003-10-14 收到，2004-05-24 改回
国家自然科学基金(60273064, 69802006)和广东省科技计划(粤财企[2001]367, A1030201)资助项目

钥注册服务规范(X-KRSS), XKMS 规范给出了客户端的请求消息和服务器端的响应消息格式、元素说明及相关计算公式等。2002 年 8 月发布了 XKMS 2.0 版，该版本在 X-KRSS 中增加了重发服务功能。W3C 组织还在不断地对该规范进行修改完善，2003 年 4 月的修订版是目前的最新版本。

2.1 X-KISS

X-KISS 即密钥信息服务规范，它用于处理与 XML 签名规范及 XML 加密规范有关的密钥信息或公钥服务的一种协议，它的主要功能包括查询所需要的公钥和描述与这些密钥绑定在一起的信息。

X-KISS 查询服务（Locate service）用于查询用户的公钥信息，可以通过提供与公钥相绑定的信息进行查询，也可以提供客户端的证书，由 XKMS 服务器端进行解析并返回公钥信息。

X-KISS 验证服务（Validate service）除了具有查询服务所具有的所有功能，还能得到公钥和其它一些数据，例如名字和一些扩展属性之间绑定状态是否有效地说明，并且该服务中所返回的都是和公钥相联系的有效的数据元素。

2.2 X-KRSS

X-KRSS 即密钥注册服务规范，用于管理与公钥相关的信息，它提供以下 4 种功能：注册、重发、撤销、密钥恢复，其中重发功能是在 2.0 版本中新增加的功能。

注册服务（Registration service）用于声明公开密钥与其它一些信息之间的绑定关系，该密钥可以由客户端或注册服务器产生。

重发服务（Reissue service）要求服务器端重新签发以前所做的注册声明，重发请求和注册请求采用同样的方式。用户发出重发请求的主要原因是用户希望注册服务通过PKI服务产生新的证书。

撤销服务（Revocation service）用于撤销用户以前发出的注册声明。撤销的原因包括基于安全考虑而定期更换密钥和私钥遗忘、泄漏等。

密钥恢复服务（Key recovery service）用于恢复用户在 XKMS 服务器备份的私钥信息。PKI 系统通常仅备份和恢复用户用于加密目的的私钥。

请求认证服务（Request authentication service）用于验证请求消息是否可信的一种机制，这种机制是符合信息安全策略的，不同于其它任何未经证明的验证机制，就其本质而言，该协议应该支持各种机构或个人发来的请求。

3 基于 XKMS 的 PKI 服务的设计

3.1 系统开发环境

XKMS 服务器端与客户端均采用 Java 语言开发，系统配置等数据以 XML 格式的文档存放，系统适用于 Windows，Linux 和 Unix 等多种主流操作系统平台。服务器端子系统发布为 Web Services/SOAP（Simple Object Access Protocol，简单对象访问协议），在 Apache Tomcat 应用服务器的支持下运行，客户端和服务器端以 SOAP 协议进行通信。

3.2 系统设计

图 1 为基于 XKMS 的 PKI 服务的体系结构图。整个系统分为服务器端和客户端两个子系统，服务器端遵循 XKMS 规范，实现了 X-KISS 和 X-KRSS 功能，包括查询服务、验证服务、注册服务、重发服务、撤销服务、密钥恢复服务等功能。所实现的这些功能以 Web Services/SOAP 的形式予以发布。客户端为用户提供了一个操作平台，将用户输入的信息按照 XKMS 的格式生成请求消息发给服务器端，接收服务器端的返回消息并从中提取有效信息予以显示。

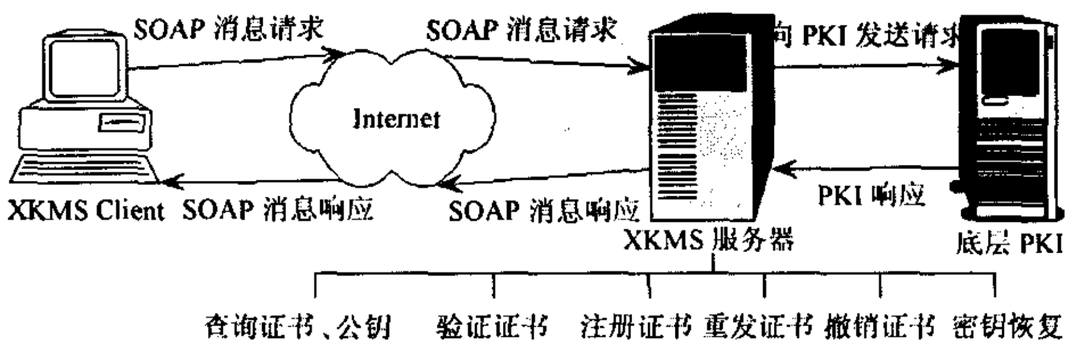

图 1　系统体系结构

服务器端和客户端之间采用 SOAP 协议进行通信，客户端采用远程过程调用（Remote Procedure Call，RPC）对服务器端发布的 XKMS 服务进行远程调用。XKMS 服务器再调用底层 PKI 开放的 API 完成相应的服务。它们之间的通信对用户来说是透明的，用户只需理解 XKMS 服务器端发布的功能。本课题组也实现了全功能的底层 PKI，限于篇幅，本文不再赘述。

详细设计方面，我们设计实现了 X-KISS 所涉及的查询服务、验证服务及 X-KRSS 所涉及的注册服务、重发服务、撤销服务、密钥恢复服务。以下以 X-KRSS 中的注册服务为例加以说明：

注册服务将用户的公钥和用户其它信息绑定在一起发送给 XKMS 服务器，申请签发属于该用户的数字证书。注册服务可以申请两种类型的证书：个人证书和服务器证书。

申请个人证书需要提供姓名、单位名称等信息，申请服务器证书需要提供按 PKCS＃10 格式[7]编码的证书请求。接收到用户的注册申请后，认证中心需要验证用户的身份。然后再判断是否给用户签发数字证书。注册完成后客户端将显示是否成功的提示信息。图 2，图 3 所示分别是本系统设计的注册服务中的客户端及服务器端的处理流程。

4 系统运行实例、测试分析

整个系统的测试在局域网中完成，客户端和服务器端分别在不同的机器上运行。计算机硬件配置为

客户端：CPU 为 Pentium 4，1.7G 的 PC，内存为 256M，

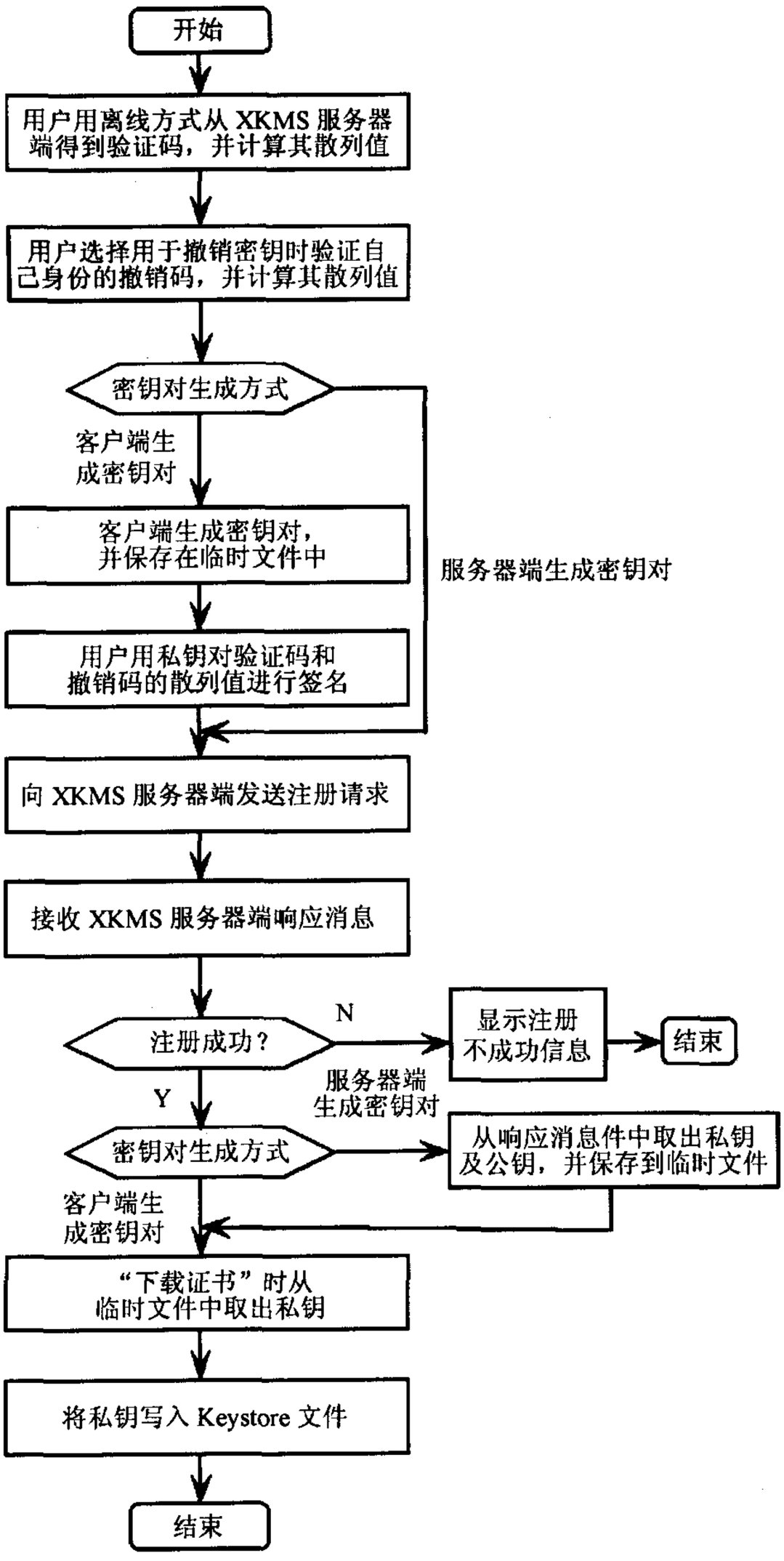

图 2 注册服务中的客户端处理流程

操作系统为 Windows 2000。

服务器：PC 服务器， CPU 为 Xeon 2.0G，内存为 512M，操作系统为 Red Hat Linux 8.0，另外安装了 Apache Tomcat 应用服务器。

经实际运行、测试表明，整个系统具有较好的性能。系统采用模块化设计，有利于系统的维护、升级。此外，系统开发采用 Java 语言和 XML 数据格式，具有很好的跨平台特性，可以很方便地移植到其它操作系统平台。

5 小结

W3C 发布的 XKMS（XML 密钥管理规范）在保持 PKI 优势的同时，降低了 PKI 部署的难度和成本。XKMS 利用基于 XML 的协议取代了传统 PKI 复杂的协议和数据格式，使客户端可以通过 XML 接口创建基于 PKI 的可信服务，避免了传统 PKI 接口的复杂性。XKMS 可分为 X-KISS 和 X-KRSS 两大部分，可分别提供查询、验证、注册、重发、撤销、密

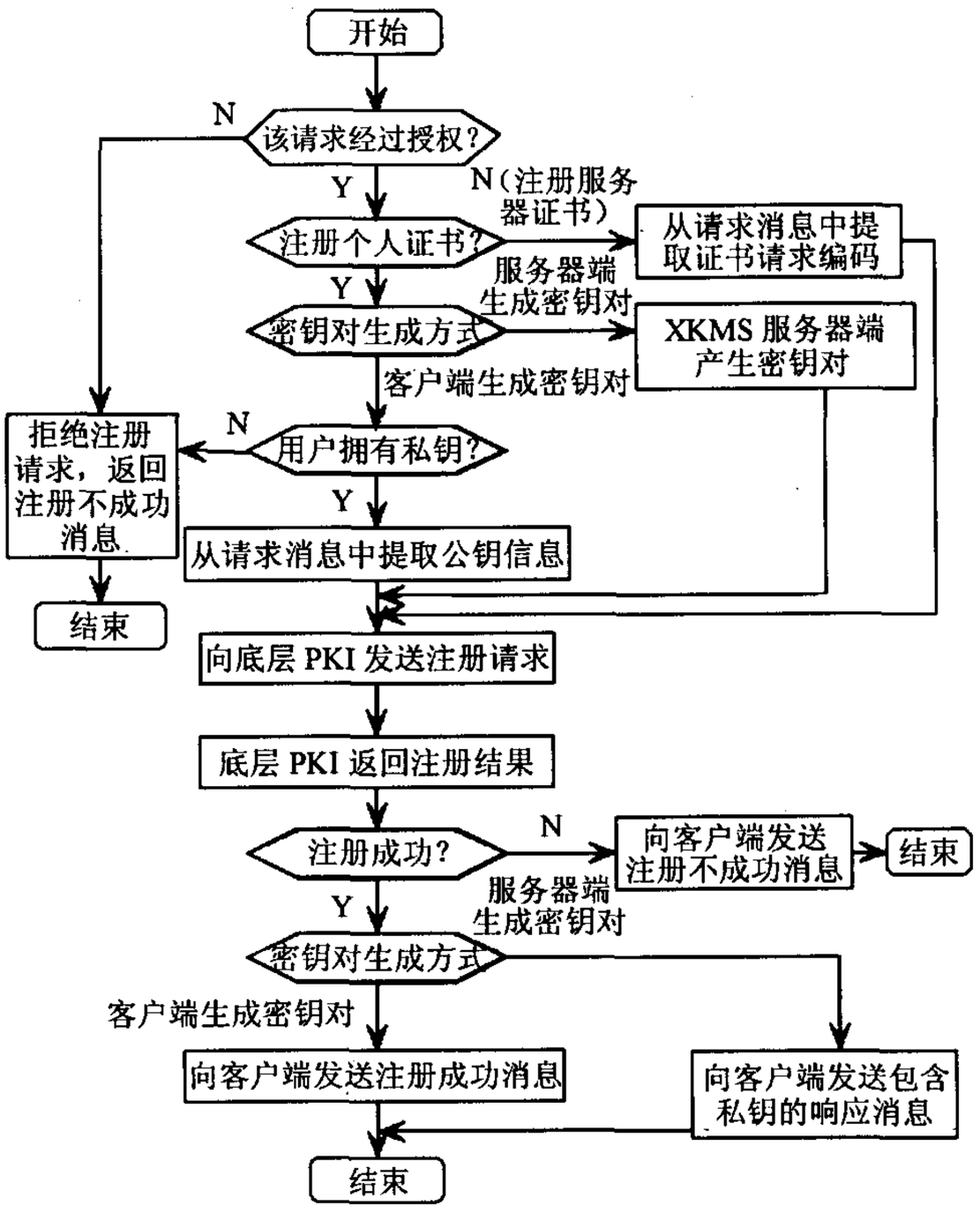

图 3 注册服务中的服务器端处理流程

钥恢复和请求验证等服务。XKMS 可以在客户机到客户机、服务器到客户机、服务器到服务器等连接中实施。本文详细介绍了本课题开发的基于 XKMS 的 PKI 系统，可以提供基于 XKMS 的 PKI 服务，经实测及分析表明，该系统运行效率高，具有跨平台、可移植性好等特性。

参 考 文 献

[1] W3C Recommendation. XML Key Management Specification （XKMS）2.0. April 2003. http://www.w3.org/TR/xkms2/ .

[2] W3C Recommendation. Extensible Markup Language (XML). Oct 2003. http://www.w3c.org/TR/REC-xml.

[3] 张剑青，刘旭东，怀进鹏. 基于 XML 的密钥管理的研究与实现. 计算机研究与发展，2003，40(1): 75－80.

[4] W3C Recommendation. SOAP Version 1.2 Part 0: Primer. June 2003. http://www.w3.org/TR/soap12-part0/ .

[5] W3C Recommendation. SOAP Version 1.2 Part 1: Messaging Framework. June 2003. http://www.w3.org/TR/soap12-part1/.

[6] W3C Recommendation. SOAP Version 1.2 Part 2: Adjuncts. June 2003. http://www.w3.org/TR/soap12-part2/.

[7] RSA Laboratories. PKCS #10 v1.7: Certification Request Syntax Standard. May 26, 2000. ftp://ftp.rsasecurity.com/ pub/pkcs/pkcs-10/pkcs-10v1_7.pdf.

唐韶华： 男，1970年生，博士，副教授，主要研究方向为信息安全.

甘志勇： 男，1975年生，硕士生，主要研究方向为信息安全.