一种基于 DSML 的证书验证方案及其实现

李寅东　郭义伟　马　宏
(NDSC 信息工程大学　郑州 450002)

摘　要　XKMS 将是下一代的 PKI 实施方案，但是它还不够完善。在与底层 PKI 进行交互时，发挥其基于 XML 的特性，使用 DSML 简化 XKMS 中证书验证机制，不失为一个更为简洁和面向未来的可行方案。

关键词　DSML，XKMS，LDAP

A DSML-based Scheme and Implementation for Certificate Validation

LI Yin-Dong　GUO Yi-Wei　MA Hong
(NDSC, Information Engineering University, Zhengzhou 450002)

Abstract　XKMS will be the next generation scheme on PKI deployment, but it is not developed enough. When an interaction occurred with lying PKI, it may be a more compact and future-oriented scheme to predigest certificate validation in XKMS, which bring feature of XML- based into play.

Keywords　DSML, XKMS, LDAP

1　引言

随着信息技术的不断进步，电子商务、电子政务的发展势头迅猛，信息安全成为广受关注的重要问题，PKI 作为信息安全的主流技术，在一定范围内得到了较好的应用，但是由于 PKI 体系庞杂，且将很多工作交给客户端去做，带来了互操作性、可扩展性差，系统维护困难等不利因素，从而阻碍了 PKI 的更广泛应用，为此 W3C 提出了 XKMS(密钥管理标准规范)，在 PKI 提供者和应用程序之间建立抽象层，为客户端提供密钥服务，实现了 XKMS 与传统 PKI(Traditional PKI, TPKI)的无缝连接，简化了客户端的实现，有利于进一步推广 PKI 技术的应用。但是 XKMS 规范没有定义 XKMS 操作如何与底层的 PKI 交互，本文拟通过 DSML 目录服务标记语言访问改进的 LDAP 目录服务，简化与底层 PKI 的交互，并达成证书验证的即时性。

2　XKMS

2.1　XKMS 概述

XKMS 是由 Microsoft, VeriSign, WebMethods 三家公司共同提出并由 W3C 所发布的 XML 安全标准之一，与 PKI 技术将所有的证书验证和查询工作完全抛给用户不同，XKMS 将用户端应用程序的 PKI 的复杂性抽象到了一个受信任的第三方 XKMS 服务。XKMS 通过与传统 PKI 服务进行接口，降低了客户端应用程序开发和部署的复杂性。XKMS 包括两个部分：(1)XML 密钥信息服务规范(XML Key Information Service Specification, XKISS)，定义了密钥定位和密钥验证两种服务；(2)XML 密钥注册服务规范(XML Key Registration Service Specification, XKRSS)，定义了密钥的注册、重新发布、撤消及恢复等服务。

2.2　XKMS 的验证机制

在 XKMS 服务中，客户端生成验证请求发送给 XKMS 服务，XKMS 服务接受到请求后，将请求消息解析，将请求内容转换为相应的验证请求与指定的基于 ASN.1 语法的 PKI 提供者进行交互，然后将结果转换成基于 XML 的应答验证消息返回给客户端。客户端解析收到的验证应答消息，完成验证。XKMS 的优点在于无论底层是怎样的 PKI 实现，PGP、X.509、还是 PKIX，在终端的用户看来，他们获得的验证服务都是一样的，不必关心低层 PKI 的不同。

3　LDAP

目录服务是按照树状结构组织信息，实现信息管理和提供服务接口的一种方法，用来定位、命名和描述网络中具有结构化特征的数据。与关系型数据库不同的是，它不支持关系型数据库中批量更新所需要的事务处理能力，一般只执行简单的更新操作，这避免了关系型数据库类型验证和事务完整性确认而引起的系统整体性能降低和系统管理烦琐等问题。目录服务被优化为针对大量的查找或者搜索操作进行快速的响应，简化了对数据的操作，适合于大容量查询。目录服务的这一系列特点使其成为 PKI 中实现数字证书及相关信息的存储、管理和查询的首选方案。轻量级目录访问协议(Lightweight Directory Access Protocol, LDAP)起源于 X.500 目录访问协议 DAP，是目前应用最为广泛的目录访问协议。

4　DSML

4.1　XML

XML 是互联网联合组织(W3C) 创建的一组规范，以便于软件开发人员在网页上组织信息，但其目的不仅在于满足不断增长的网络应用需求，同时还希望通过 XML，能够确保在通过网络进行信息传输时，具有良好的可靠性与互操作性。

XML 是一种数据描述、定义语言，使用者可以定义任意的标记来描述文件中的任何数据元素，使文件的内容更丰富、更复杂并组成一个完整的信息体系。由于它的开放性和自描述性，使得它成为 Internet 上共享信息的最佳途径和应用程序之间交换数据的最佳媒介。

由于 XML 能针对特定的应用定义自己的标记语言，因此 XML 可以在各种领域中一展身手，根据不同的系统、厂商提供各具特色的独立解决方案，只要应用程序能够理解 XML 中的标记就行。而 DSML 便是 XML 在目录服务方面的具体

应用。

4.2 DSML

在 Web Service 环境下，应用程序自身的运行功能和调用方法都是通过 XML 形式进行描述与展现的。而传统的目录服务有其专有协议，如 LDAP 不支持这种形式的请求，目录服务标记语言(DSML)的出现提供了一种解决办法，它提供了以标准 XML 文档的形式表现目录请求和操作的方法。通过 DSML，目录的信息能被基于 XML 的应用使用，扩展了 LDAP 目录的到达范围。

5 XKMS 证书验证设计方案

5.1 现有证书验证方式的不足

尽管 XKMS 以 Web 服务的形式向用户提供了新一代密钥管理的服务，降低了客户端应用程序开发的复杂性，用户可以将繁复的证书操作交由 XKMS 服务去做，只需要请求相关服务和得到结果，但是 XKMS 服务现实情况下并不是独立于传统 PKI，它仍然要与传统 PKI 服务进行交互。

对证书验证服务来说，通常是由 XKMS 与 PKI 网关进行交互，获得请求证书的验证信息。若 XKMS 服务器内部维护的证书库没有所要查询的证书信息，它就必须与底层的 CRL/OCSP 进行交互，以获得待验证的证书信息。这种交互需要在 XKMS 中实现对底层 PKI 的验证协议接口模块，针对不同验证机制的接口模块设计仍是较为复杂的。

而底层的 CRL/OCSP 验证机制也存在其局限性，CRL 是定期发布的证书撤消列表，而证书撤消是随机的，这种滞后性不能满足验证证书即时状态的需求。OCSP 对出错信息不予签名，使得攻击者可以伪造出错信息发送给客户端，对客户端进行拒绝服务攻击。

5.2 本文的证书验证设计方案

XKMS 证书验证机制的设计与实现来源于笔者所在的研究部承担的网络监管系统研制项目中监管网安全子项目，基于 DSML 的验证方案简化了与底层 PKI 的交互，同时也较好地保证了验证的即时性和证书链的验证。

考虑到 XKMS 的目标之一是提供一种基于 XML 的简单协议，以便通过 XKMS 服务处理密钥信息，使应用程序不必理解复杂的 PKI 语法和语义。在与传统 PKI 交互中，基于 XML 的处理具有同样的优势。使用目录服务标记语言(DSML)，可以以 XML 形式与存放证书信息的 LDAP 目录交互以获得证书相关信息。但 LDAP 也要适当地设置以配合 DSML 方式的证书验证。我们考虑对 LDAP 目录进行一定的改进以利于 DSML 直接请求相关的证书信息，以完成数字证书的验证。

为了提高 XKMS 服务的处理速度，获得即时的证书撤消信息，在 LDAP 目录服务中取消 CRL 的存储，在 LDAP 目录服务中的每个存储证书消息的条目中都设置一个 Boolean 状态属性来标记证书有无被撤消，CA 签发证书后，向 LDAP 目录服务器发布证书，并将此状态属性值设置为 True；当用户提出撤消申请并被 RA 审核后，CA 将此证书所在条目中的此状态属性值改为 False。在检验证书时，只需读取该证书所对应的状态属性值。CA 对 LDAP 目录有读写权限，DSML 请求信息只能读取 LDAP 目录信息，请求信息都以 XML 加密和签名，确保传输过程中的安全性。

进行验证时，XKMS 服务器发送请求信息至 LDAP 目录服务器，LDAP 目录服务器返回响应消息，包含请求验证证书的状态属性值和签署 CA 证书，以及签署 CA 的上一级 CA 的 LDAP 目录服务器地址，状态属性值和上一级 CA 的 LDAP 目录服务器地址使用 CA 私钥签名。

返回的证书状态属性值在 XKMS 服务器解析后，若为真，则对签署 CA 同上进行验证，发送验证请求到上一级 CA 的 LDAP 目录服务器验证 CA 证书状态，直至到达被信任的根证书，完成验证，向客户端发送证书有效响应信息。过程中当 LDAP 返回的响应消息中证书状态属性值为假时，立即终止余下的验证，向客户端返回证书无效消息。证书链的验证过程见图 1。

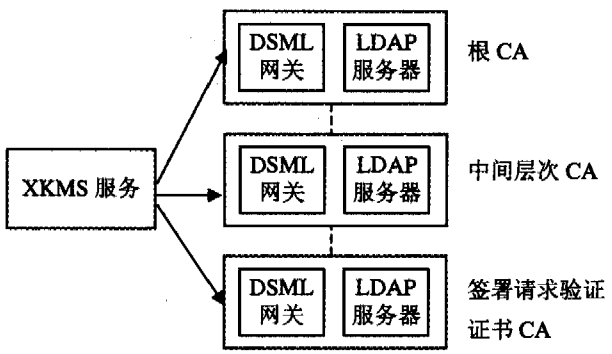

图 1 证书链验证示意图

6 证书验证方案的实现

验证方案的实现使用 Weblogic server 作为 Web 服务器，加载 XKMS 服务，目录服务器采用 OpenLDAP，DSML 解释程序的实现则使用 Exolab 的 Casor API，目录服务通过 DOM 方式访问 DSML 文档，对目录服务器的访问使用 JNDI API。

当用户端的证书验证通过 SOAP 消息请求 XKMS 服务时，XKMS 解析请求消息，将有关参数传递给 Java Servlet 程序。Java Servlet 将参数转化为对应的 DSML 文件传送给 DSML 解释程序，解释程序通过 JNDI(Java Naming and Directory Interface)向 LDAP 服务器发出请求，LDAP 服务响应请求，返回请求验证证书的状态信息。解释程序将得到的结果再转化成 DSML 文件，传回到 XKMS 服务，XKMS 服务程序解析返回的结果，并将验证结果以响应信息发送给客户端，实现简略图如图 2 所示。

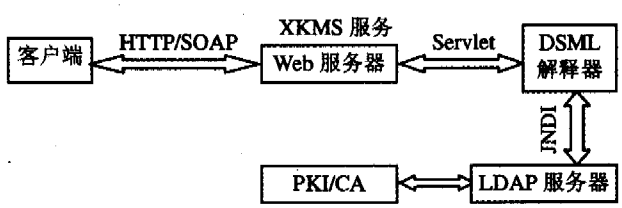

图 2 基于 DSML 的证书验证方案实现略图

本设计方案是在 XKMS 与传统 PKI 结合的基础上，针对证书验证服务进行专门的优化设计，从而无需在 XKMS 中实现传统 PKI 验证协议接口模块，加密的 XML 格式消息易于被同样基于 XML 的 XKMS 解析，简化了验证过程，同时实现了证书验证的即时性和证书链的验证。

参 考 文 献

1 W3C Recommendation. XML Key Management Specification (XKMS 2.0) Version2.0. http://www.w3.org/TR/xkms2/. 28/06/2005
2 DSML Specification 1.0[EB/OL]. http://www.dsml.org
3 郭一鸣，沈剑，陆松年. 基于 DSML 的 Web 目录服务系统的设计与实现. 计算机应用研究，2005(1)
4 The OpenLDAP Project. OpenLDAP Software 2.3 Administrator's Guide[EB/OL]. http://www.openldap.org/doc/admin23/