# 改进的LDAP服务体系及其在电力系统PKI中的应用

张少敏，史占成，郭雅薇，王保义

(华北电力大学计算机系,河北 保定 071003)

**摘要**：随着电力系统信息网络建设的迅速发展，信息安全问题日益重要。PKI技术是目前广泛采用的安全解决方案，而轻量级目录访问协议LDAP是PKI技术的重要组成部分。针对传统LDAP系统负载过大，往往造成网络的堵塞的缺点，提出了改进的LDAP服务体系结构设计方法，并详细讨论了电力系统PKI中改进的LDAP服务体系的设计原则及其实施的总体的框架。此体系结构采用分区模式，在一定的同级LDAP区域中达到负载均衡。实例分析的结果证明了该方法的可行性。

**关键词**：信息安全；公钥基础设施PKI；轻量级目录访问协议LDAP

## Improved LDAP service architecture and its application in PKI of electric power system

ZHANG Shao-min, SHI Zhan-cheng, GUO Ya-wei, WANG Bao-yi

(School of Computer, North China Electric Power University, Baoding 071003,China)

**Abstract:** With the rapid development of information networks in power systems, information security is becoming more and more important. PKI is a solution of security adopted widely, and LDAP is an important part of PKI. Aiming at the insufficiency of traditional LDAP service structure that a heavy load will lead to jam of networks, an improved LDAP service structure is proposed. The design principle and realization framework are dealt with in detail. The framework adopts the pattern of subarea, and load balancing is achieved among the LDAPs at same level. In the end, a practical example to realize the new framework in power system is given to prove that the improved LDAP server system is feasible.

**Key words:** information security; PKI; LDAP

中图分类号：TM76　　文献标识码：A　　文章编号：1003-4897(2008)08-0073-03

## 0 引言

随着电力系统信息网络建设的迅速发展，网络信息安全问题日益重要，而PKI（Public Key Infrastructure）技术是目前各国广泛采用的安全解决方案。它是通过公钥密码体制中用户私钥的机密性来提供用户身份的唯一性验证，并通过数字证书的方式为每个合法用户提供一个合法性的证明[1]。目录服务系统LDAP是PKI的重要组成部份，其主要功能是数字证书、证书废除列表CRL的发布、更新、查询。

## 1 LDAP简介

目录服务是用一个特殊的数据库存储资源信息，将各种资源信息在目录树结构中分层存储，提供一个单一的逻辑视图，允许用户和程序透明地访问网络上的各种资源[2,3]。LDAP主要优点如下：简单而通用，已广泛用于各种主流和非主流的计算平台；LDAP目录易于理解；由于LDAP的高可靠性和良好性能，LDAP目录服务能满足绝大部分重要的目录服务需求，已经成为目录服务的事实上的标准。对于需要从不同的地点读取，但是不需要经常更新的数据，使用LDAP存放是最佳的方案。因此在PKI体系中被广泛应用于证书、CRL信息发布。

## 2 改进的LDAP服务体系

### 2.1 传统LDAP服务体系结构

在传统的PKI体系中，通常只有1套LDAP系统，包含主从互为备份的2台服务器，所有查询、验证都是通过这套LDAP系统提供。但是随着PKI/CA系统的发展，数字证书用户越来越多，基于证书的业务应用也越来越多，这个时候，再用单一的LDAP方式工作，常常会造成LDAP系统的负载过大，同时往往造成网络的堵塞[4]。传统的LDAP服务体系结构

基金项目：华北电力大学重大项目预研基金（20061302）

如图 1 所示。

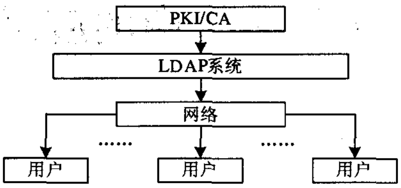


图 1 传统的 LDAP 服务体系结构

Fig.1 The traditional service architecture of LDAP

### 2.2 改进的 LDAP 服务体系结构

本文提出了一种改进的 LDAP 系统，它能很好地解决传统 LDAP 系统的问题。改进的 LDAP 服务体系结构如图 2 所示。

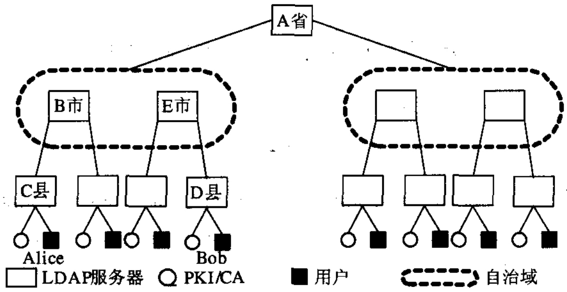


图 2 改进的 LDAP 服务体系结构

Fig.2 The improved service architecture of LDAP

在改进的 LDAP 系统中，PKI / CA 系统只与本地的 LDAP 系统发生关系，CA 系统签发完证书或是证书废除列表 CRL 后，只需将证书或是 CRL 发布到本地的 LDAP 上即可，本地 LDAP 会自动地把证书或者 CRL 推到其上一级 LDAP。对于每个 LDAP 系统，只需和一个父 LDAP 系统相连，如果用户查询本地 LDAP 没有找到要验证的证书，该 LDAP 将向其父 LDAP 发出证书请求，如果父 LDAP 也没有所要验证的证书，系统将对父 LDAP 所在自治域内的其它 LDAP 进行查找，如果没有找到，该 LDAP 将继续向其父 LDAP 发出证书请求，直至最后查到相应证书位置，然后将该证书放入本 LDAP 系统，再下载到用户手中。

例如，用户 Alice 在 A 省 B 市 C 县，则 CA 系统在给该用户签发完证书后，将其证书信息分别放到 C 县的 LDAP 服务器上，C 县的 LDAP 服务器会自动地把证书推到 B 市 LDAP 服务器上，B 市的 LDAP 服务器会自动地把证书推到 A 省 LDAP 服务器上。用户 Bob 在 D 县，当其要查询 C 县 Alice 的证书，在 D 县 LDAP 系统上找不到该证书时，则去 E 市 LDAP 系统上找证书，如在 E 市 LDAP 系统上还是没有找到，则在 E 市自治域中进行查找，此时在自治域中 B 市 LDAP 中找到 Alice 证书，这样就不用去 A 省的 LDAP 系统上去找了。

在图 2 中，假如某用户在 A 省 LDAP 服务器上也没有找到要验证的用户证书的信息，则说明要验证的用户的证书不存在。该 LDAP 服务方式与 PKI /CA 系统没有任何关联，可以在任何时候挂接到 LDAP 服务系统中去，同时也不受已有的 LDAP 服务系统的限制，可以挂接到任何一个 LDAP 层次，甚至再增加一个层次。由于证书可自动查询，用户还可以对该系统进行优化，如对于长期不用的证书可以放到一边，这样就可以极大地提高证书的查询速度。

## 3 改进的 LDAP 在电力系统中的应用

### 3.1 改进的 LDAP 目录服务系统的总体框架

在电力系统 PKI 体系中，改进的 LDAP 目录服务系统的设计应遵循如下原则：

① 在相对独立的用户管理区域内部署本地的目录服务器，本地目录服务器提供本地用户信息的查询；

② 对本地的信息采取推方式向上一级 LDAP 复制用户信息，可以防止某级 LDAP 中的数据遭到破坏而导致的用户证书信息的丢失；

③ 加强各级 LDAP 的安全设计，防止用户证书信息被利用、篡改或删除。

基于上述设计原则，电力系统 LDAP 目录服务系统的总体框架如图 3 所示。首先，在国家电力公司部署 LDAP 目录系统，存储、管理各省的用户信息、证书信息等；其次，各级节点的 LDAP 目录系统采用主从服务器设计方式，保障该节点目录服务的可靠性；最后，在相邻省、市之间，建立一定范围的自治域，使用户不必再经过上级 LDAP 系统就能查询到其它地区的用户证书。

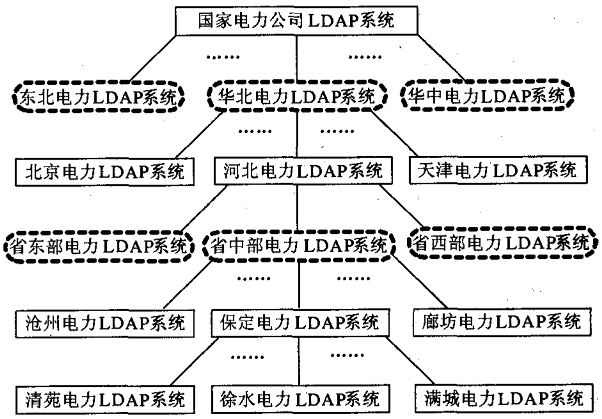


图 3 电力系统 LDAP 目录服务系统

Fig.3 The directory service system of power system LDAP

### 3.2 LDAP 系统的安全设计

LDAP 目录服务系统安全性设计的目标是：防止对任何资源进行未授权的访问；保护数据的机密性、完整性和非否认攻击；如果目录服务器的数据遭到侵害，可以及时、有效地恢复所有数据。

访问控制的目标就是防止对任何 LDAP 目录服务中的资源进行未授权的访问。虽然 LDAP 目前并无具体的有关访问控制的标准，但从一些草案中或是现实已被使用的 LDAP 产品的采取的访问控制策略，它们都是基于访问控制策略语句来实现的，同时 LDAP 还提供很复杂的不同层次的访问控制，它是通过基于访问控制列表来实现的，无论是基于组模式还是角色模式，都摆脱不了这种限制。

为了保护数据的机密性、完整性和非否认攻击，需要在客户端与服务器端之间建立安全的请求与响应。为了达到这个目的，双方之间的通信需要在安全通道或接口上进行。目前，在 LDAP 中提供了基于 SSL/TLS 的通讯安全保障。SSL/TLS 是基于 PKI 的信息安全技术，LDAP 通过 StartTLS 方式启动 TLS 服务，可以提供通讯中的数据保密性、完整性保护。通过强制客户端证书认证的 TLS 服务，同时可以实现对客户端身份和服务器端身份的双向验证。为了建立 SSL 链接，需要在 LDAP 服务器上指定具体的端口号。通常使用 636 作为 LDAP 的标准 SSL 端口号来进行 TCP 或 UDP 通信。

由于 PKI 对 LDAP 目录服务器系统有高可用性和高安全性的要求，如果只采用单一服务器系统显然无法满足系统的这些要求。可以采用基于服务器的双机双控容错系统，2 台服务器共同工作，当一台服务器的系统出现故障时，另一台服务器可确保系统正常运行，从而将系统风险降低到最低限度。双机双控容错系统有 2 种工作模式。

① 主机和从机都有完全独立的系统，从机的备份系统提供对主机的实时备份，当工作站在提交任务时，同时提交给主机和从机。主机与从机之间有心跳监测，一旦从机发现主机心跳停止，立即宣布接管主机，在接管过程中会有半分钟左右的宕机时间。

② 主机与从机有独立的操作系统与独立的数据服务，但是数据存放在同一个外部磁盘阵列设备上。主机与从机的数据服务同步，主机与从机之间有心跳监测，一旦从机发现主机心跳停止，立即宣布接管主机，接管过程没有宕机时间。

考虑到电力系统用户的实际需求，可采用第 2 种方式对 LDAP 目录服务系统进行双机热备份。在整个网络系统中 2 台服务器加 1 台磁盘阵列柜及 1 套双机热备份软件构成双机热备份系统，做到数据共享及集中管理，能够 7×24 h 保证系统正常运行。

## 4　结语

随着电力行业信息化的不断发展，我国必将大力推动 PKI 在电力系统中的应用。基于改进的 LDAP 系统的设计方法能保证目录服务系统的安全稳定运行，因此会有非常广泛的应用前景。

### 参考文献


[1] Laurent-Maknavicius M.A PKI Approach Targeting the Provision of a Minimum Security Level within Internet [A].In:Fourth European Conference on ECUMN'07[C]. 2007. 433-438.

[2] 余勇,林为民.分布式 LDAP 及其在电力系统 PKI 中的应用[J].电力自动化设备,2005,25(11):44-47.
YU Yong, LIN Wei-min. Distributed LDAP and Its Application in PKI of Electric Power System[J]. Electric Power Automation Equipment, 2005,25(11):44-47.

[3] 杨燕,顾君忠.联邦式.LDAP 目录服务系统的研究与实现[J].计算机应用,2004,24(6):159-161.
YANG Yan, GU Jun-zhong. Design and Implementation of Federated LDAP Directory System[J]. Computer Applications, 2004, 24(6): 159-161.

[4] Hornfeldt J, Heumann M, Wilson W P,et al.An Enterprise Application Architecture for Electronic Government[A]. In:23rd Annual Conference on LCN'98[C].1998.270-277.


**收稿日期**：2007-08-23；　　**修回日期**：2007-11-13

**作者简介**：

张少敏（1965-），女，教授，主要研究方向为电力信息网络及电力市场信息安全；E-mail: zhangshaomin@126. com

史占成（1981-），男，硕士生，主要研究方向为电力信息网络及电力市场信息安全；

郭雅薇（1982-），女，硕士生，主要研究方向为电力信息网络安全。