



成功案例

国家某部委信息中心 PKI/CA 安全服务器

2002 年 6 月 8 日

项目背景：

该部委信息中心是一个涉密单位，在各省会城市均有子系统，网络应用复杂，对信息安全有很高要求。在这次 PKI 项目实施之前，系统内部大量使用 Unix 和 Windows 系统，费用昂贵，且 Unix 系统的通用型不强，在主机升级时面临重复的软件投资，而 Windows 系统从稳定性到安全性均不能满足要求。

该网络中有 Web、Email、数据库等多种服务器，以及专用的办公系统，多台 PC 计算机作为工作站，为了有效利用网络资源，提高办公效率，做到人员权限的有效管理，保证在应用过程中的安全性，该中心使用了基于 PKI（Public Key Infrastructures）/ CA（Certification Authority）技术的身份认证的安全方案，网络中的各种应用服务如 Email 和 Web 等都可以利用这种强制有效的认证手段来对使用者的身份和权限加以鉴别。并使用专门的硬件加密产品保证加密传输和 PKI 证书生成中的复杂运算。

客户需求：

CA 和目录服务器使用两台浪潮的 PC 服务器，另外有一台硬件加密机来负责证书生成中的复杂运算。这样，CA 服务器成了该应用系统的中心，如果它出了安全问题，不但影响正常的使用，而且会对全系统的安全带来隐患。所以必须保证 CA 服务器的安全，需求包括：CA 服务器本身的正常运行、CA 的配置文件、数据库安全、CGI 程序的安全、系统有防火墙、审计日志等。

从管理上，要求有对超级用户的限制，应用与操作系统、应用与应用之间做到安全隔离，有安全审计作为监督机制。

因此，使用达到国家标准要求的安全操作系统，是 CA 服务器所必须的安全保障。

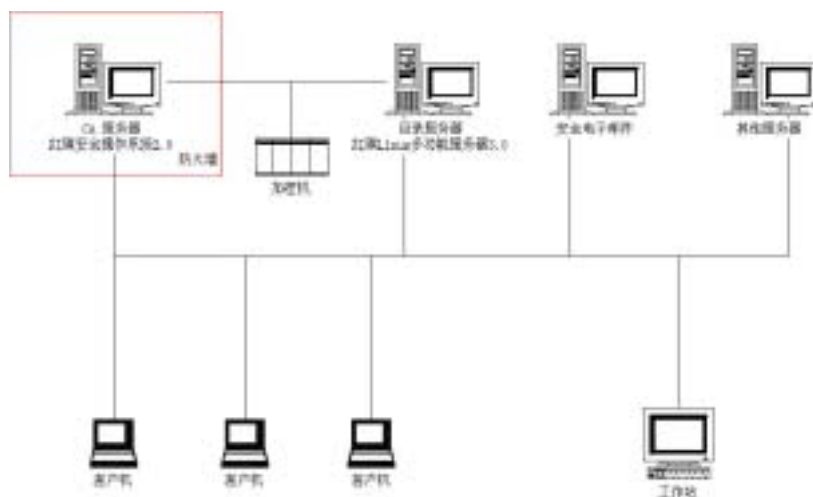
解决方案及部署实施：

为满足客户的需求，红旗软件针对应用特点，和开发商配合，提出了相应的项目解决方案，使用两台服务器，分别作为 CA 中心和目录服务器，CA 中心使用达到国标第三级（B1 级）的红旗安全操作系统 2.0 版，目录服务器使用红旗多功能服务器 3.0。





成功案例



网络拓扑图

在 CA 服务器上，重点对客户应用程序和数据库进行支持 and 安全保护，同时使用防火墙屏蔽无关的端口。CA 服务器上配有两块网卡，一块通过防火墙和局域网相连，另一块和加密机相连，目录服务器也有两块网卡，分别和局域网以及加密机相连。

在 CA 服务器上，运行有 PKI 的用户注册、证书生成和管理、权限设定等应用，使用红旗安全操作系统 2.0 特有的三大安全特性，保证了上述这些应用的安全：

- 1、安全操作系统保证了从管理上实现三权分立，系统管理员、安全管理员、审计管理员共同承担操作系统的最高权限，避免单个人对整个系统的控制；
- 2、只有 mysql 用户启动的 mysqld 服务程序能访问 mysql 数据库的数据文件、配置文件和日志文件，其他用户（包括 root）和进程无法直接访问这些文件，提高了数据库的保密性和完整性；
- 3、只有特定用户才能运行 CA 服务程序，使用自主访问控制和强制访问控制，其他用户（包括 root）不能篡改 CA 应用的资源；
- 4、使用完整性强制访问控制，保护系统命令、CA 应用程序、Web 页面及图形、系统底层连接库、核心算法以及主要配置文件不被破坏和替换；
- 5、使用核心提供的软件防火墙，保护必要的服务端口，关闭所有无用的端口；
- 6、系统核心有健全的安全审计功能，可记录一切涉及安全的事件，并有专门的审计管理员来监督系统安全事件，并可以配置审计事件范围。

在目录服务器上，运行 LDAP 服务，作为日常使用时的证书发布系统。使用红旗 Linux 多功能服务器的目录服务，高效易用易管理。同样配置了防火墙，保护必要的服务端口，关闭所有无用的端口。

北京中科红旗软件技术有限公司

中国北京海淀区万泉河路 68 号紫金大厦 6 层，100086

电话：8610 - 82656655 传真：8610 - 82658096

[Http://www.Redflag-Linux.com](http://www.Redflag-Linux.com)





成功 案例

效果评价：

客户使用了红旗安全操作系统产品以及安全配置方案，完成后的系统可以满足客户对安全的需求，运行稳定可靠，通过技术实现了在管理上的多权分立，避免单人对系统的控制，同时保护了关键资源的保密性和完整性，CA 中心得到了系统的良好支持以及安全保护，目录服务器可同时面向应用系统中的大量用户提供稳定的服务。而应用开发商在开发和系统集成过程中，得到了红旗软件方面良好的支持和定制，无需修改源程序，所有安全配置都可以通过脚本来部署，快速方便。

北京中科红旗软件技术有限公司

电话：8610-82656655

传真：8610-82658096

网址：<http://www.Redflag-Linux.com>

地址：中国北京海淀区万泉河路 68 号紫金大厦 6 层

邮编：100086

本材料最终解释权归北京中科红旗软件技术有限公司所有

北京中科红旗软件技术有限公司

中国北京海淀区万泉河路 68 号紫金大厦 6 层，100086

电话：8610 - 82656655 传真：8610 - 82658096

[Http://www.Redflag-Linux.com](http://www.Redflag-Linux.com)

