铁路运输管理系统
网络安全项目
方案建议书

商业机密

Sun Microsystems of California Limited.

2002 年 11 月

版本

版本	描述	日期	作者
2.0	第二版稿	2002 年 11 月 11 日	Jing Ming Li Ray Cheng 乔智君 周涛 吕艳平 许禹 张诚（神州数码）

目录

1. 概论

1.1 背景

铁道部计划建立一个现代化的、安全可靠的、面向服务的网络系统。Sun 公司专业服务部向铁道部提交一个可行的安全解决方案，提供网络用户认证、应用程序访问控制、机密性和不可抵赖性服务、反病毒、入侵检测和物理安全等各级安全功能。

本建议书提出了纵深的安全方案以及实现的组成部分和服务。本方案包括了 Sun 公司的硬件、软件产品以及 Sun 专业服务部门提供的专业咨询服务。

Sun 是提供网络计算的硬件、软件和服务等方面的业界领先的供应商，总部位于加州北部硅谷地区的中心地带。Sun 公司在 170 多个国家和地区运营，每年的营业收入超过 180 亿美元。Sun 为用户提供最好的安全产品，从 Solaris 操作系统到世界领先的 PKI 管理和用户管理产品。

Sun 专业服务部作为 Sun 企业服务部门的三个业务分支之一，提供技术咨询和系统集成的专业技术，帮助企业以最佳的设计实现企业电子商务解决方案。Sun 专业服务部 提供与安全相关的咨询服务，从安全架构的设计到具体实施。

1.2 技术环境

铁道部具有包括总部在内的 63 个业务单元。目前存在的问题主要是：整个网络结构基本上是扁平的；没有网络分区划分；没有基本的网络基础架构。

网络结构：

由于计算机网的建设是伴随各个应用项目的建设和要求逐步扩展的，投资方式也是分步、分期的，不可能开始就有一个整体规划，故而缺乏保护层次，呈平面型结构。平面结构网络规模增长到一定程度后，管理难度增大。

业务混合的控制

网络的特性允许各应用数据组合传输，而且为提高设备利用率各应用系统共用通道也

是合理的选择。无论从各网络应用业务或网络传输管理本身，对混合业务的控制还缺乏有效的手段。从资源的使用考虑，对混合业务的网络及信息资源的访问，缺少有效的访问控制机制。

局域网设备介绍

铁路系统的部、路局和分局 63 个机关园区网的结构基本上是平面结构，设备主要有 3COM 和 Cisco 公司的产品。

广域网设备介绍

铁路系统计算机广域网的结构基本上是平面结构，骨干网的通道速率一般为 2Mbps，设备主要有北电和 Cisco 公司的产品，网络路由协议采用 OSPF 和 RIP。

应用系统

大部分用户信息包含在本地应用程序中，没有集中的用户管理机制。

软件产品

铁道部已经购买了 Netscape Directory Server、Application Server 和 CMS 系统（均为 1999 年以前版）。CMS 是可运行的系统，可以发布证书。然而，这些证书还没有在实际中运用起来。

1.3 项目目标

铁道部网络安全项目的目标是建设一个先进的网络安全体系架构，为铁道部提供安全可靠的计算和通讯环境。规范网络基础，形成纵深保护层次，提高网络自身抵御攻击的能力和网络整体性能，满足日益发展的应用系统数据传输和安全要求。

另外，铁路计算机网络承载较高级别的敏感信息，根据国家保密局的建议，参照涉密网的标准建设。

具体内容包括：

- 以外部防火墙、网络物理隔离系统和内部防火墙为基础，将网络调整为外部服务网、内部服务网和安全生产网的纵深防御框架体系；

- 以 PKI/CA 和代理机制为基本技术建立网络访问控制机制、建立统一的用户管理和授权管理体系及相关的 DNS、用户目录体系；
- 在新的框架体系下集成病毒网关和既有的入侵检测、漏洞扫描软件；
- 同时构建较为完善的日志及日志分析系统。
- 配置通用的 PKI 系统，结合 PKI 的应用系统集成；

Sun 公司专业服务部将与铁道部及合作伙伴紧密配合，设计并实现该系统。

1.4 方案综述

Sun 公司专业服务部将与铁道部及合作伙伴紧密配合，设计和实施世界级的安全系统。该系统包括分层以及纵深的边界防卫体系，对铁道部应用系统基于角色的安全的访问控制。

对于边界防卫系统，Sun 公司将与铁道部指定的供应商协调工作，设计最佳的安全策略和流程，建立可行的安全架构和框架，如分层防火墙架构、反入侵检测和响应系统、反病毒和 Web 代理系统等。Sun 服务器的技术水平保证了最高的扩展性、可靠性和稳定的计算平台。**Sun 可以为铁道部提供 Solaris 源代码，在铁道部与 Sun 之间的许可证协议保证下，用于评估、研究和开发等目的。**

边界防卫只是整个安全框架的一个组成部分。并且，安全系统应以方便安全的方式将对数据和应用系统展现给适当的用户。按用户在铁道部中的角色，可以设定他们对应用系统的访问策略。Sun 公司提供的铁道部应用系统安全解决方案使用了基于开放标准的世界级的技术和产品。本方案的基础是 **Sun ONE LDAP 目录服务器(Directory Server)，是迄今为止最可靠、最具扩展性的目录系统，应用在了许多世界级的公司中。**

在该目录服务器之上，本方案使用了 Sun ONE 身份服务器（Identity Server）和 Sun ONE 证书管理系统（Certificate Management Systems）。Identity Server 帮助铁道部构建集中式的访问策略，执行在铁道部的应用系统和其它 Web 资源中。Sun ONE Identity Server 也是业界第一个支持 Liberty 标准和 SAML(Security Assertion Mark Language)的产品。SAML 为跨组织的单点登陆（Single sign-on）提供了标准的方式，提供了用户简档共享的方法。Liberty 规范基于 SAML，刚于 2002 年 7 月发布。Sun 公司的 CMS 系统为发放和管理 X509 公钥证书提供了标准的方法。作为市场上最早的 CMS 系统，Sun ONE CMS 是成熟、稳定、经过大量实践考验的产品。

作为整个解决方案的组成部分，Sun 公司有经验的技术架构师和咨询顾问将与铁道部

的软件和系统工程师一同工作：

- 建立铁道部 CA 系统
- 使用 Sun ONE 目录服务器建立集中式的用户管理系统
- 建立集中式的策略和访问控制机制
- 对铁道部应用系统的改造，使之可以利用 PKI 作为其认证与访问控制方式

应用系统的改造将基于 Mozilla 开放源代码安全项目。Mozilla 开放源代码安全项目是 Netscape 浏览器 SSL 功能的基础，广泛用于 Sun 和 Netscape 的许多产品中。**通过 Mozilla 源代码，铁道部可以获得 SSL 和其它加解密功能的源代码。这对于铁道部进一步发展应用系统级的安全能力是非常有益的。Mozilla 源代码包括 Java 和 C/C++接口。**

Sun ONE 设计的也提供了应用系统内容的聚集，内容的个性化服务以及从 Internet 对应用系统的安全访问等。

下面的章节将深入描述 Sun 公司提供的铁道部安全解决方案。

2 企业级安全架构综述

2.1 方法论和最佳实践

要建立安全的网络系统，必须首先了解什么是网络系统的安全性，以及有哪些因素威胁着网络系统的安全。

国际标准化组织(ISO)对计算机安全有精确的定义，其内容主要包括两个方面：即物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于被破坏和丢失。逻辑安全包括信息完整性、保密性和可用性：

- 保密性 指高级别信息仅在授权情况下流向低级别的客体与主体。
- 完整性 指信息不会被非授权用户修改,并且能保持其一致性。
- 可用性 指合法用户的正常请求能及时、正确、安全地得到服务或回应。

由于大型网络系统内部运行的各种网络协议(TCP/IP、IPX/SPX 等)并非专为安全通讯而设计。所以，网络系统可能存在多种安全威胁：

1、软件系统的安全问题

这中间包括操作系统、防火墙以及应用服务本身所存在的安全隐患。

2、来自网络的安全性问题

例如，客户的系统可能无法对来自 Internet 的电子邮件挟带的病毒及 Web 浏览器可能存在的恶意 Java/ActiveX 控件进行有效控制。此外，还有来自企业内部的攻击。

要防止这些威胁给网络系统带来危害，安全的系统应具备以下基本功能:

- 良好的访问控制

通过为特定网段和服务建立严格的访问控制体系，将绝大多数攻击拒之门外。

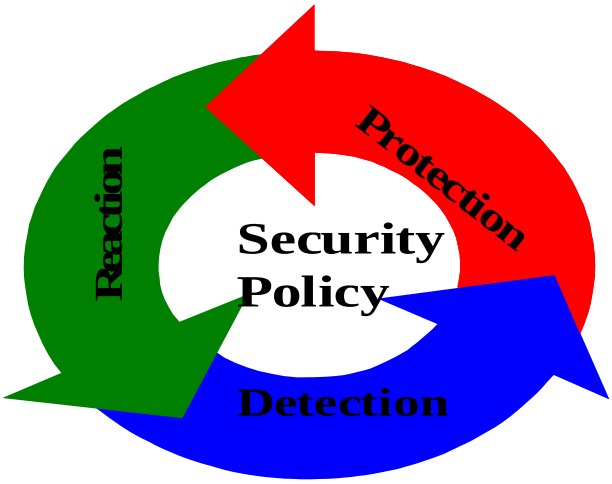
- 检查安全漏洞

即使攻击者攻击到了目标，通过对安全漏洞的定期检查，也可使绝大多数攻击无效。

- 备份和恢复

良好的备份和恢复机制可在攻击造成损失时，尽快地恢复数据和系统服务。当然,保证物理层的安全可靠是整个系统安全可靠运行的基础。

如何监控和防止黑客对网络和系统的入侵是系统安全建设一个难题。目前采用的安全模型是可适应网络模型，即 PDR。PDR 模型如下所示，通过完善 PDR 模型的某一方面来达到对黑客入侵的响应与防卫。



其中： P（Protection）即防护，通过访问控制、口令、授权、防火墙等保护手段来保护网络和系统的安全。D（Detection）即安全检测，通过扫描和实时监控技术来检测网络和系统的安全漏洞、黑客攻击检测等。R（Reaction）即安全反应，对网络和系统的漏洞、黑客入侵等所应采取的动作。

安全是企业网络和计算环境的基础。内部网络、外部网络、大量的分布式C/S系统和Web服务给组织增加了保护企业资源的风险。常见的威胁包括：

- 身份窃听
- 伪装
- 回放攻击
- 数据窃听

- 操纵
- 争议
- 病毒
- 拒绝服务
- 恶意的移动代码

为应付这些威胁，需要下列安全服务及产品：

- 认证
- 访问控制
- 数据机密性
- 数据完整性
- 不可抵赖性
- 内容过滤
- 入侵检测

我们应该知道，达到适当的安全级别是一个长期和不断前进的过程。简单依靠购买、安装和配置一些提供安全服务的产品，是远远不够的。铁道部各单位应充分理解影响网络和信息安全的威胁，理解如何克服这些威胁的服务手段，了解实现必要服务的架构，明晰制定安全策略的主要因素。

规划和实现网络安全并不是一个纯粹的技术问题，它依赖于业务种类、可用资金状况和建立适当安全策略。用户是任何网络安全系统的基础，因此需要对用户进行适当的培训，确保对安全需求和管理过程有正确的认识。

成功的网络安全系统也意味着可以有效的方式，让合法的用户有效地访问适当的资源。这就要求在网络的安全性和用户使用的方便性之间达到某种平衡，网络安全系统也应尽可能实现对用户透明。

达到这种平衡的一个主要因素就是系统支持单点登陆(Single Sign-On)。访问电子邮件、数据库系统等其它服务时，以对用户透明的方式顺利通过认证。

作为中长期规划，建议铁道部系统的网络安全体系的设计也应采用这一动态自适应模型的设计思想，将门户系统的安全管理看作一个动态的过程，安全策略应适应网络的动态性。动态自适应安全模型由下列过程的不断循环构成：安全分析与配置、实时监测、报警响应、审计评估。

（1）安全分析与配置

在构建系统时，从一开始就要从整体上考虑系统的安全性。这包括以下内容：标识和认证、存取控制、密码技术、完整性控制、审计和恢复、操作系统安全、数据库系统安全、防火墙系统安全、计算机病毒防护和抗抵赖协议等等。安全分析与配置阶段就是要全盘考虑上述问题，给出相应配置。具体来说包括下面步骤:

- 系统分析阶段：如系统风险分析、系统安全需求分析、安全管理条例、安全标准、应用系统规格和数据应用分类。
- 计划阶段：如软件和硬件平台选择、系统用户权限的划分、内部子网互联方式的选择、安全屏蔽系统的确定、系统安全策略的制定、安全系统软件性能的评估和系统实施时间表的制定。
- 实施阶段：包括 Web 服务器、应用服务器、数据库服务器等各种服务器的配置，系统性能配置，安全管理配置和安全规则文件配置等等。

（2）实时监测

实时监测网络攻击模式和其他网络可疑活动，这包括:

分析黑客行为、病毒特征、系统弱点，提取出数据特征，作为实时监测的知识库和方法库，以便实时监测网络攻击和病毒模式，及时发现系统弱点和漏洞。例如可将攻击行为分为四类:拒绝服务、攻击前预探测、非授权访问、解码等；系统弱点和漏洞可分为十三类:简单邮件传输协议类、强力攻击、守护进程、网络远程调用、NFS 网络文件系统/X Windows、服务拒绝、NetBIOS 类扫描、NT 系统、代理/域名系统、WWW 服务、IP 欺骗、防火墙、文件传输协议等。

通过对各种网络服务和应用协议的分析，找到各类服务的正常数据流格式和应用方法，作为系统可疑行为知识库，以便实时监测可疑的网络和系统操作。

根据系统安全规则，建立系统违规行为分析知识库，实时识别网络和系统违规行为。

（3）报警响应

对发现的各类攻击模式、系统弱点和漏洞、病毒、违规行为、泄密等各种威胁，系统给予相应的响应，包括：

- 记录相关信息的日志；
- 通过控制台消息、E-mail、页面调度程序发出警告；
- 阻断非法连接；
- 调用用户自定义的策略程序；
- 上述这些响应的组合。

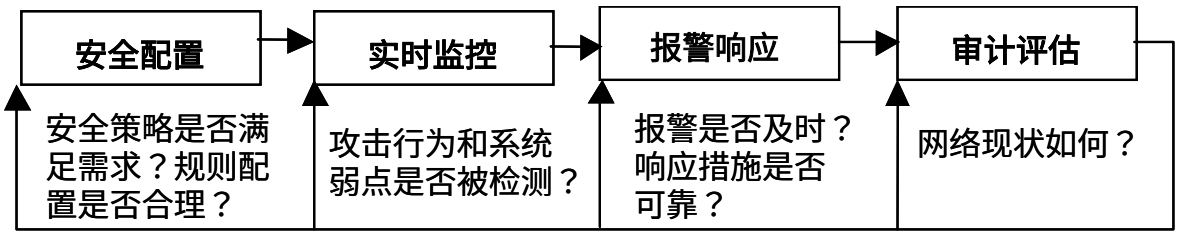
（4）审计评估

审计评估的目的是根据网络的报警记录、日志信息及其他信息向管理员提供各种能够反映网络使用情况、网络上的可疑迹象、网络中发生的问题等有价值的统计和分析信息，运用统计方法学和审计评估机制给出智能化审计报告及趋势报告，综合评估网络安全现状，并把它作为下一次循环的输入状态。

审计是模拟社会监察机构在计算机系统中用来监视、记录和控制用户活动的一种机制，它使影响系统安全的访问和访问企图留下线索，以便事后分析和追查。其目标是检测和判定对系统的恶意攻击和误操作，对用户的非法活动起到威慑作用，为系统提供进一步的安全可靠性。

审计是现代安全计算机系统必不可少的组成部分。它在身份鉴别、访问控制、数据完整性、加密技术等多种安全措施的基础上,进一步提高了系统的可信性。目前，计算机审计记录已具有法律效力。

下图表示了网络安全模型的循环过程及各过程中的反馈。

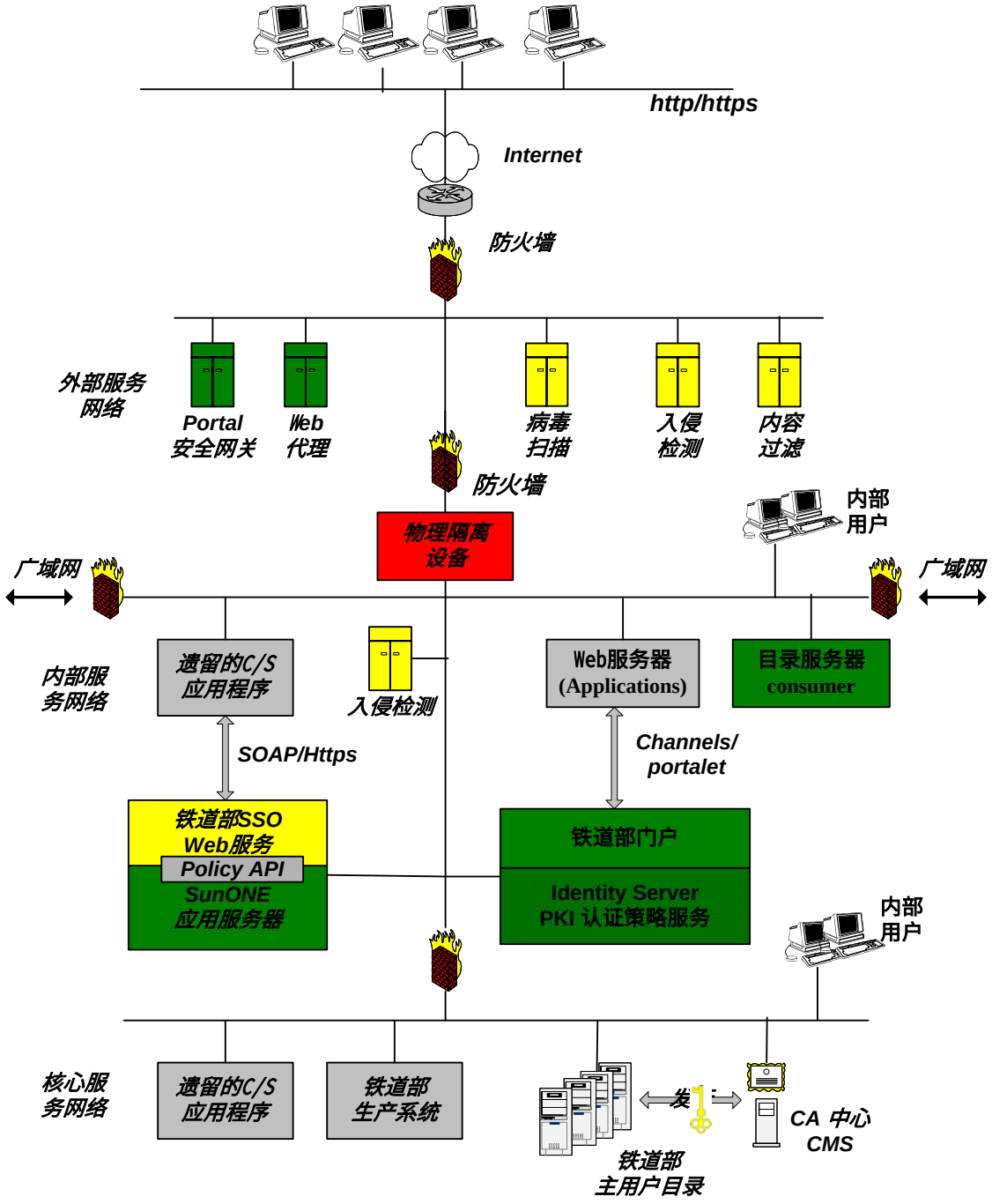


网络安全模型

上述模型中每一个子过程都有可能反馈。因为，在每一过程的检验和确认阶段都可能发现问题，只有不断反馈才能达到理想状况。整个过程不断循环，Internet 安全才能不断达到新的台阶。

2.2 安全架构

安全的架构请参见下图：



2.3 安全策略

安全策略是整个安全体系的基石，为用户、系统管理员和经理人员提供一系列可遵循的规范和限制条件。企业提出经过规划的可执行的规章制度，所有员工都应认真履行，避免对安全的责任和限制各自为政。在本方案建议书中我们只概述了两个安全策略，当然还有许多其它的安全策略，如邮件的使用、Web 浏览器的使用等。

2.3.1 用户安全策略

用户安全策略详细描述用户对可支配的技术资源的责任和限制。用户对计算机资源的访问必须加以限制。举例来说，安全策略可能规定用户不能改动未指派使用的计算机的硬件设备。另一个例子是，安全策略规定用户不能安装操作系统，除非得到系统管理员的帮助或者相关经理的认可。

2.3.2 系统管理员安全策略

系统管理安全策略详细描述系统管理员的责任和限制。这些责任和限制与计算机资源及用户有关。举例来说，安全策略规定系统管理员不允许在任何服务器上安装脚本，除非有至少两个其它系统管理员或者一个管理代表的对脚本的理解和认可。

2.4 基础设施级的安全性

2.4.1 防火墙, DMZ 和网络隔离

网络设计应考虑利用对信息的访问控制来规避风险，这是非常关键的。直接将数据暴露给不可信的网络如 Internet，是非常危险的。同样重要的是应与其它可信区域隔离开来，如将管理网络和核心数据网络相隔离。

2.4.1.1网络隔离

安全设计应考虑按层次隔离信息。象 Internet 这种不可信的网络，对企业信息应没有任何直接的访问权限。对企业信息的访问只能通过允许的网络应用程序进行，如通过 Web 服务器。此外，在网络之间必须将可信区域隔离开。每个可信网络应该由访问控制系统管理，如防火墙等。这些访问控制点在隔离的网络间扮演“门”的角色，控制何种信息可以在网络之间进出。

2.4.1.2 DMZ

企业可以用 DMZ 区域部署自己的 Internet 服务，而同样保证未经授权的行为不能访问它的私有网络。DMZ 位于 Internet 和内部网络的保护线之间，通常结合了防火墙和堡垒性主机。典型情况下，DMZ 包含了可访问 Internet 通信量的服务器，如 Web 服务器、FTP 服务器、Email 服务器和 DNS 服务器等。

2.4.1.3 防火墙

防火墙的作用是在隔离的网络间阻止未经授权的访问。当对 Internet 可以完全透明的访问时，防火墙可以用作保护企业内部网络的安全。防火墙也可阻止未经授权的内部用户访问敏感的网络资源。这样，所有进入或者离开隔离网络的消息都必须通过防火墙，防火墙检查每个数据包是否满足网络安全的准则。

为了适应客户的网络流量要求，保证网络性能，防火墙实施中要考虑采用双机方式的高可用性技术和进行负载平衡。

防火墙被认为是保护私有信息的第一道屏蔽。

按访问技术划分，有三种类型防火墙：

- 包过滤防火墙：检查每个进出网络的数据包，根据用户定义的规则决定接受还是拒绝。包过滤对用户是相当有效和透明的，但难以配置。另外，它容易受到 IP 欺骗的影响。
- 应用程序防火墙：在指定的应用程序上实行安全机制，如 FTP 和 Telnet 服务。它是非常有效的，但可能会导致性能的降低。

- 链路级防火墙：当 TCP 或者 UDP 连接建立后，应用安全机制。一旦创建连接，包可以在主机之间流动，不需要进一步的检查。

2.4.2 代理服务器

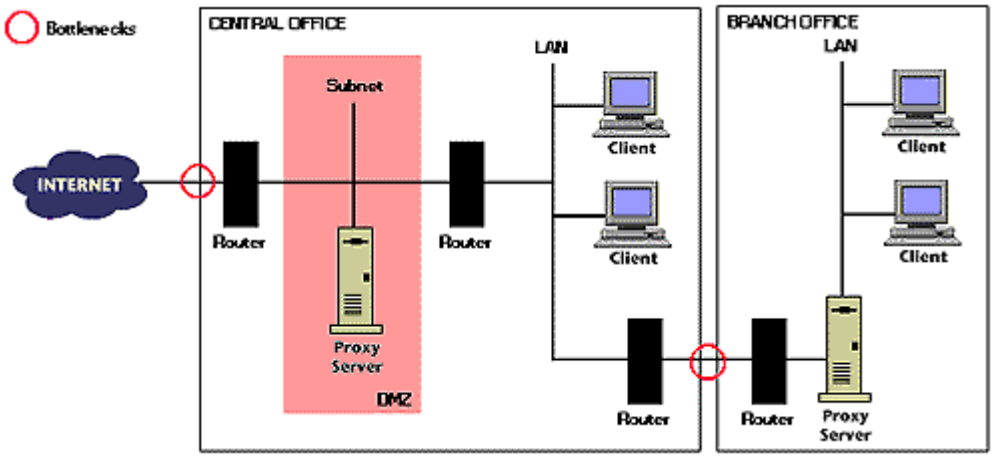
部署代理服务器可对内部资源提供额外的保护。代理服务器可以通过以下方式改善网络安全：

- **代理：** 代理服务器可提供内部客户端通过防火墙对 Internet 的访问。该服务经常作为 Intranet 安全策略一部分的方式提供，即“正向代理”。前向代理允许铁道部客户端通过防火墙访问外部，而不影响私有网络的完整性。服务器也可以提供外部客户端通过防火墙对内部内容的访问，该服务经常用作 Web 安全发布，即“反向代理”。

- **过滤和访问控制：**代理服务器可从 Intranet 内对 Web 内容提供细密的访问控制。网络管理员可以使用过滤器阻止访问任何 Internet URL 或者去改变实际的内容流。使用访问控制列表，过滤器可以用于特定的地址、地址组、单独的用户或者用户组。

- **日志：**服务器将记录所有的错误和访问信息。日志为网络管理员和小组经理提供有用的信息。网络管理员经常分析日志文件，来监控服务器的性能和使用状况。组经理将感到基于日志的报告在追踪其员工 Internet 使用状况时是非常有用的。

Sun 咨询顾问可提供架构咨询服务，包括设计正确的代理架构，根据需要设计代理插件，并帮助实施等。一种可能的代理服务器的实现方式参见下图，中心 Offices 和分支 Offices 为缓存和安全目的，都部署了代理服务器。

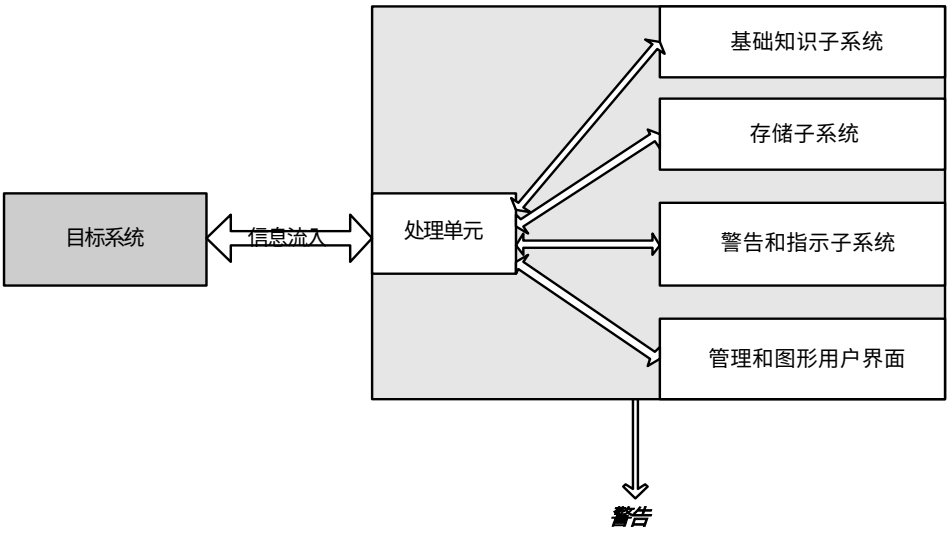


2.4.3 入侵检测系统

入侵检测系统以实时的方式，监控网络和识别可疑的通信量并向管理员提出警告。实时地识别可疑或未经授权的行为是非常重要的，可以识别和减轻安全威胁。

有可能在发生恶意或者未授权的行为时，企业并不知晓。对攻击的忽视客观上纵容了攻击者不断地去尝试，如果攻击不能有效地被检测和阻止，攻击者可能迟早会得手。

入侵可定义为某些恶意方采取的一系列相关的行为，导致了对计算机或网络系统的安全威胁。入侵检测系统(IDS)的架构参见下图：



过程子系统实现了入侵检测算法，也包括常用的系统管理功能，是入侵检测系统的核心。例如，为了检测对 Internet 标准协议(Telnet, HTTP, SNMP, SMTP)的攻击，在过程子系统中需要有一个协议声明的转换引擎

基础知识子系统包括：

- 用户的行为和活动模式，比如登陆和注销时间、使用的服务、使用的命令和 CPU 利用模式等
- 系统行为，如最高 CPU 加载周期、各种服务器的 CPU 利用模式、服务器内存和磁盘的利用状况等。

- 签名和字符串，如某些文件名、某些术语（如“铁道部所有”）和一些服务的名称

过程子系统按照入侵检测算法，与基础知识子系统一起进行检查。

存储子系统存储大量的过程子系统的数据。

警告和和指示子系统在某些入侵事件发生时，决定是否发送警告通知和采取行动。

2.4.3.1 网络入侵检测

通常情况下，建议将基于网络的入侵检测系统部署在所有的隔离网络上。网络入侵检测系统的目的是识别可疑的行为，并在危害发生前向管理员提出警告。应该说明的是，基于网络的入侵检测系统不能监控加密的通信量。

2.4.3.2 基于主机的入侵检测

基于主机的入侵检测系统应维护一个文件系统和数据完整性的数据库。当系统的执行或配置文件被发生修改时，该数据库可起到验证的作用。数据库应以安全的方式离线存储。数据库应该在每周都进行更新和验证，或者只有当修改发生时进行。

2.4.4 病毒检测和内容过滤

病毒检测服务器可以扫描电子邮件消息(SMTP)、网页内容(HTTP)和文件内容(FTP)。为提高性能，我们可在不同的服务器上分担扫描任务。例如，一个扫描服务器可以扫描 SMTP 和 FTP 流，而另一个服务器专注在 HTTP 上。

病毒检测的核心是扫描引擎。扫描引擎同时使用模式匹配技术和基于规则的内容扫描技术。引擎可以处理压缩的数据格式，举例如 Base64,、Quoted Printable 和 Uuencode。由于字处理软件的宏也是常见的病毒来源，扫描引擎分析这些宏判断是否具有恶意性。类似地，如果没有有效的证书和签名，引擎可以检测和拒绝 ActiveX 和 Applets。

2.4.5 物理隔离

国家保密局发布的《计算机信息系统国际互联网保密管理规定》第六条规定：“ 涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行物理隔离 ”。

这条规定在目前国内信息与网络安全技术还不够发达，而网络攻击与犯罪又日趋严重的情况下，对于保护涉密网络安全是一项很有效的措施，有重要的现实意义。

在实施了物理隔离之后，必须解决涉密网络的用户访问因特网的问题。物理隔离系统解决方案的目标就是在保证涉密网络和因特网的物理隔离的前提下，使涉密网络用户能够访问因特网。

安全物理隔离系统通常包括专用物理隔离切换装置、数据暂存区等部分，同时也可以采用防火墙技术、基于内核的入侵检测技术、安全操作系统内核技术和离线式邮件转发技术、智能离线浏览技术以及病毒扫描与清除技术等多种安全技术，组成从内部网络到因特网的安全数据交换通道。

物理隔离系统最基本功能包括隔断从因特网到专网内部的网络连接，仅允许数据暂存于数据暂存区中，做到在任何时间都没有因特网到专网内部的网络物理连接。为了提高网络连接安全性，物理隔离系统通常还会集成其它安全功能，包括实时的入侵监测，使用安全操作系统，使用安全的应用服务程序，对暂存在缓冲网络中的数据，包括邮件的内容、附件和压缩附件中的文件等数据进行全面的病毒扫描、清除和报警，防止因特网上的恶意 IP 包进入隔离系统等。

2.4.6 加密

加密保证数据传送的安全性。这减少了关键数据和认证源数据被监视的风险，确保数据的完整性。

（1）经由网络的加密

为确保信息的加密性，应该对流动于不可信网络间的敏感数据加密。如 SSL 和 SSH。有的企业 SSL 的负荷很重，建议采用 SSL 硬件加速器来改善性能。

（2）远程管理的加密

所有的对远程系统的管理访问必须加密，如在管理和生产系统间的 SSH 或者 IPSec 通道。

2.4.7 服务器和网络设备安全

2.4.7.1硬件补丁和操作系统

通常情况下，补丁包放置在公共邮件列表或设备供应商的公告板上。通过这种方式，系统管理员能够及时获得操作系统和硬件的最新补丁包和安全警告。

操作系统和硬件设备上的安全漏洞应尽快加以弥补，可利用最新的补丁程序，或采取其它临时的替代性方法，确保组织中的所有机器都保持在最新的安全状态上。

2.4.7.2平台安全性

主要是利用供应商发布的安全更新和补丁程序弥补操作系统和平台中的漏洞。对每个平台也可以指定一些安全程序，如口令破解程序，anti-nuke 程序，完整性验证程序和基于主机的入侵检测程序等。进一步而言，企业的安全策略应规定在自身网络上允许运行哪些平台和服务。

2.4.7.3路由器

必须配置路由器去执行一系列规则，提供第一层抵制攻击和减少防火墙负荷的作用。然而，这种方式的弊端是一些攻击企图将不能记录在防火墙的日志上，因为路由器会阻止他们。由于路由器没有防火墙的日志和警告功能，攻击的起因将可能因此而被忽视。

2.4.7.4网络设备和端口

网络设备和端口用于 C/S 和 TCP/UDP 架构上。在服务器和客户端之间，这些服务和

端口实现了多种不同的协议。在许多服务器上，遗留着一些不需要的、没有用处的，甚至是不知道的服务，都通过一定的端口存在着。举例来说，存在一些系统管理员不知道的远程过程调用，暴露了机器和软件系统的状态，这是非常危险的。这些没有使用的端口对于有经验的恶意攻击者而言，是很有利用价值的。攻击者经常扫描机器端口，希望发现这样的端口存在。如果有，他们就通过入侵一个机器从而攻击网络内其它对它可信的机器。

2.4.8 日志和警告

日志维护何时发生和发生什么的审核记录。日志可以标识出安全裂缝何时发生，或者正发生着可疑或恶意的行为。当这些事件发生时，警告主要人员。可以识别行为和减轻风险。系统不仅在本地记录日志，而且应记录在安全的远程日志服务器上。这样确保当系统被入侵，仍然有安全的审核机能。另外，集中式的日志管理简化了日志的监控和评估。如果系统被入侵和损害，系统和应用程序的日志将是不可信任的。此外，如果对日志不进行监控，未经授权的访问行为依然可能没有被检查。

安全的远程日志服务器应专注于对企业系统的记录。由于服务器的作用在于聚集和评估日志，应具有高度的安全性和专用性。日志也应以只读格式存储。路由器、Unix 系统、交换机等都应记录在远程系统上，记录的信息包括：

- 无效的认证
- 成功的认证
- 会话开始
- 会话结束
- 系统活动

日志通常可于 30 天内访问，超过 30 天后的日志应以物理安全的方式离线存储。

对日志应做到每日评估，全面的评估应每周进行。评估的目的是识别可疑和恶意的事件。应利用自动化工具帮助对系统的评估，在进行日志数据的评估时也可以使用第三方的应用程序。

日志系统应具备警告机制。警告机制在事件发生时通过屏幕显示、电子邮件、SNMP trap、Syslog、声音、运行报警程序、LogService 消息等方式自动通知主要的管理人员。

2.5 应用级的安全性

应用程序级的安全因素包括

- 访问控制
- 身份认证
- 单点登录
- 授权

2.5.1 访问控制

可以部署代理服务器对内部资源提供保护。代理服务器可提供内部客户端通过防火墙对 Internet 的访问，也可以提供外部客户端通过防火墙对内部内容的访问。代理服务器可从 Intranet 内对 Web 内容提供访问控制。

我们在方案中采用代理服务器实现了访问控制，请参见前面相关章节。

2.5.2 身份认证

网络上的通信双方在交易时需要确认对方的真实身份，在涉及到支付时还需要确认对方的帐户信息是否真实有效。

身份认证的常用技术包括：

1. 用户 ID 和口令

用户名/口令是最传统的认证方式，此种认证方式要与 LDAP 相结合，即用户名和口令信息存放在 LDAP 结构中。

在铁道部的应用系统中的用户 ID 和口令将构建在 PKI 系统之上。

2. Tokenk 卡

在认证的方式中可采用 Token 卡方式认证，此种方式是每个都有一个具有计算功能的 Token 卡，同时在内部有一个与 Token 相对应的认证服务器，门户服务器的认证模块要与此认证服务器相结合来实现采用 Token 卡方式的认证。采用 Token 认证方式可以做到一次性动态密码，增加了的身份认证安全性。

3. 基于 PKI 的证书系统

使用 Token 卡方式的身份认证只是对持卡人的认证，无法判断持卡人的真正身份（如在卡丢失的情况下）；而且此卡人也无法判断其锁链接的服务器就是的门户系统。要做到上述功能的认证就是采用电子证书的认证。

Sun 公司的咨询顾问将与铁道部的技术人员一同工作，构建铁道部的 PKI 系统，有关 PKI 的知识及 Sun 公司的解决方案参见第四章。

2.5.3 单点登陆

实现用户一次登陆就可以获得对多个应用程序的访问能力，在提高效率方面扮演着重要角色。在美国的研究表明，用户因为使用多帐号和多口令的麻烦，造成每年 44 个小时的浪费。同时，多点登陆也引起口令遭破坏的风险。

我们在方案中采用 Sun ONE Identity Server 及其提供的 SDK 和 API 作为实现 SSO 功能的基本框架。具体内容参见第四章。

2.5.4 授权

在企业和机构中，通常会按照等级层次关系组织用户，按用户的角色决定其授权。因此，同一层次或角色的用户有相似的访问权限。这就有效地形成了用户访问和授权机制的管理。

数据按其重要性划分。为定义不同的用户有不同的访问权限，关键业务数据需要进行分类。

网络访问权限关注于哪些用户有权限访问哪类网络服务。对某些网络服务有权限的用户而言，访问权限决定用户能读、写还是执行网络资源。

我们在方案中采用 Sun ONE 系列产品实现授权功能，具体内容参见第四章。

3 基础设施级安全架构

3.1 概述

在金融、政府、通信、制造等行业，Sun 公司提供的硬件、软件和设备极大增强了客户的安全性。纵深的网络安全体系提供了网络计算环境下最好的安全架构，采用了安全的产品、流程和规程。

隔离手段限制了恶意黑客所造成的破坏范围，延缓了攻击得手后的进展。在多级防卫层次上部署不同的安全技术，可以更有利于捕获黑客的行为。

本章中，我们首先介绍了系统的安全架构，而后描述了安全架构的方法、产品和技术。

3.2 系统化安全架构

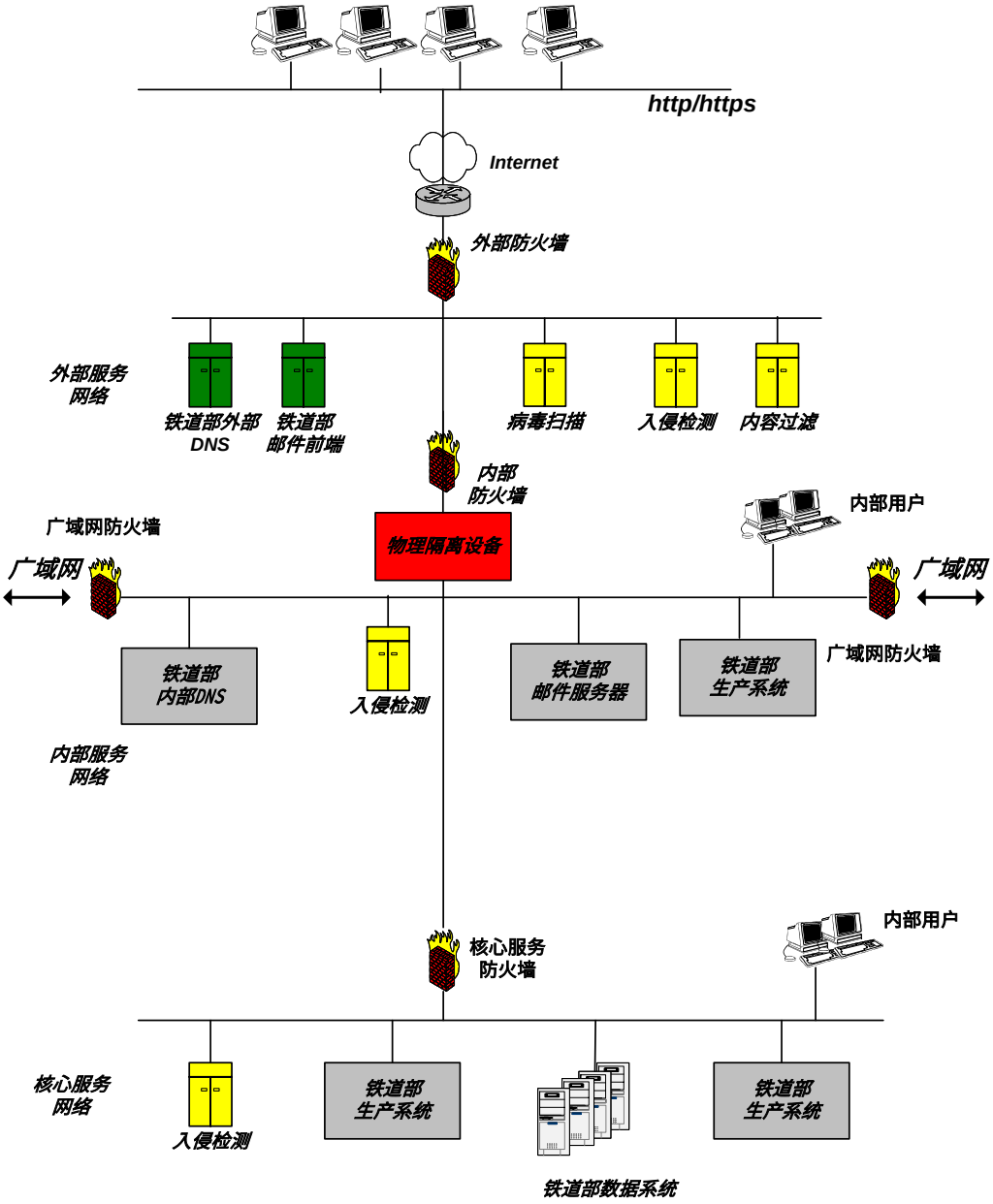
Sun 公司建议的基础安全架构基于 Sun 的经验、最佳实践以及调查研究，可以充分满足铁道部的技术需要。正如下图所示，整个网络结构分 Internet、广域网、外网、内网、核心服务网络和一系列安全产品及技术。

在图中，用防火墙阻止对铁道部外网、内网和核心服务网络资源的不合法访问。例如，外防火墙可以否决任何从 Internet 到代理服务器的 RPC 访问等。

病毒扫描产品检查所有收取的电子邮件，来检测和修理感染的邮件消息或附件。内容过滤产品主要关注对特定字符或段落的检测。入侵检测产品监控网络和服务器的被入侵状况，需要指出的是，每个网络和子网络都应受监控，即使是已由防火墙保护的网络。

图中没有明确标识出的架构组成部分还包服务器优化、完整性确认、URL 控制、审核和日志、安全策略、安全流程和紧急响应处理流程等。当文件和目录发生变化时，完整性确认可以检测出并发送警告。审核日志分析增加了检测和阻止对资源不合法访问的另外一

个级别。对铁道部用户和系统管理员而言，制定良好的安全策略帮助他们理解对公司资源可以什么和不可以做什么。安全流程进一步降低了铁道部系统管理员人为错误的可能性。即使有了最好的策略、流程和技术，我们依然应该对可能出现的最坏情况做充分的准备，当安全事件发生时，将遵循预定义的处理步骤尽量减少损失。



安全基础架构

3.2.1 广域网

铁道部的广域网目前连接着 63 个点。某种程度上，广域网在入侵和偷听上是安全的。在广域网和铁道部站点的连接点之间仍然需要部署防火墙，阻止内外部恶意的攻击。

3.2.2 Internet

为增强对铁道部大量用户的服务，允许用户能访问铁道部信息，将来还可能允许通过 Web 浏览器访问。这对铁道部及其员工是有益的，能使用电子邮件、Web 浏览器和访问其它 Internet 资源。铁道部员工可以在家中或者商务旅行中通过 Internet 访问铁道部资源，为铁道部用户提供了更好地服务，增加了生产效率。可在 Internet 和铁道部外部网络间部署外部防火墙，来阻止恶意的攻击和控制客户和员工的访问。

与铁道部的广域网相比，Internet 比较经济，Sun 建议铁道部将来在铁道部的各个点都连接到 Internet 上。

3.2.3 外部网络

能够直接从 Internet 访问的服务器部署在外部网络上，例如 DNS 服务器、代理服务器和邮件前端服务器。在 Internet 和外部网络之间的流量由外防火墙和物理隔离设备控制，而外网和内网间的流量由内防火墙控制。在外网上附加一些实现某些安全功能的服务器，如病毒检测、内容过滤和入侵检测。外网也叫做 DMZ。

3.2.4 内部网络

那些不能直接通过 Internet 访问的服务器、工作站和其它设备部署在内部网络上，例如内部 DNS 服务器、邮件存储服务器、LDAP 服务器、工作站等。根据各点的规模，在内网中可能有多个局域网。铁道部的各个内网都连接到广域网上。包含敏感或受限制信息的服务器、工作站和设备将不能放置在内网络上，而将放置在核心服务网络上。在内网和外网之间的流量由内网防火墙和物理隔离设备控制，而内网和核心服务网络间的流量由核心服务防火墙控制。在不同内网络之间的流量将穿过广域网防火墙。在内网中，也运行着入侵检测系统等。

3.2.5 核心服务网络

核心服务网络是铁道部最内部的网络，部署了最敏感的服务器、工作站和设备等。这些服务器可能是数字证书主服务器、财务应用服务器和其它敏感应用服务器等，与外部的唯一接口需通过核心服务防火墙。为进一步的防护，在核心服务网络上可以放置多个入侵检测服务器。

3.2.6 全面防卫系统

Sun 建议采用以下工具和服务来实现铁道部的全面防卫系统：

1. 防火墙
2. 物理隔离系统
3. 入侵检测
4. 完整性保证
5. 病毒防范
6. 内容过滤
7. 访问控制
8. 关键服务器系统的安全
9. 紧急响应体系
10. 日志系统与审计
11. 安全策略
12. 安全流程

3.3 防火墙

3.3.1 内容提纲

正如前面章节所述，防火墙的作用在于阻止对网络未经授权的访问。当允许对 Internet 完全、透明的访问时，防火墙起到保护铁道部内部资源的作用。防火墙也用于阻止未经授权的用户访问敏感信息或连接。

防火墙的基本原理对大多数专业人士和黑客来说比较容易理解。它的状态表追踪 TCP 会话，允许防火墙内的人员访问外部的 Internet，客户或合作伙伴访问公司信息，阻止黑客访问内部资源。

铁道部为了保持与外部的联系，必须开放一些端口和信息入口。例如，为了客户可以访问铁道部的 Web 服务器，必须开放端口 80 或 HTTP。

在 Internet 上，有许多工具可以帮助黑客利用这些条件。建议使用一个端口扫描程序 NMAP，可以扫描防火墙并发现进出网络的所有客利用端口。

3.3.2 工具

在铁道部网络系统上，部署三类防火墙。分别是外部防火墙、内部防火墙和核心服务防火墙。我们建议每种防火墙都安装在业界最稳定的操作系统 Solaris 上。

Sun 公司建议采用第三方产品，并按照不同的部署需要选择不同产品，以满足国家相关法律法规对铁道部网络安全的要求：

- 外部防火墙 – 国内公司生产的防火墙产品
- 内部防火墙 – 国内或国外公司的防火墙产品
- 核心服务防火墙 –国内或国外公司的防火墙产品

3.3.3 咨询流程

防火墙的咨询服务包括以下工作：

1．检查防火墙部署体系结构设计，包括防火墙在网络中的位置，可用性和可扩展性；

2．检查防火墙设置规则；

3.3.3.1防火墙部署体系结构检查

检查防火墙部署的位置，DMZ 体系结构，检查防火墙高可用性和负载平衡方案，检查防火墙的管理规定，如防火墙日志管理，防火墙安装区域，规则更动流程等。检查信任网络分段。

3.3.3.2 检查防火墙规则

根据铁道部网络安全策略和防火墙规则的业界最佳实践，检查防火墙规则。业界最佳实践的示例如下：

- 所有没有明确允许的都应该禁止
- 在规则集的顶端设置最通用的访问规则，明确规则应用的次序
- 尽量详细精确的定义防火墙规则
- 在同一个防火墙规则中避免使用相同的源和目的
- 最小化防火墙的规则数目，确认所有可以合并的规则均已合并
- 安装规则到特定的防火墙而不是安装到网关上
- 明确适当的定义缺省规则、标准规则
- 确保所有的出厂默认特性已经被关闭

3.4 物理隔离系统

3.4.1 内容提纲

物理隔离系统必须要考虑国家政策的符合性，以及系统的可信度。

物理隔离系统的目标是确保在不可信的外部网和内部网络之间没有物理或电子通路。

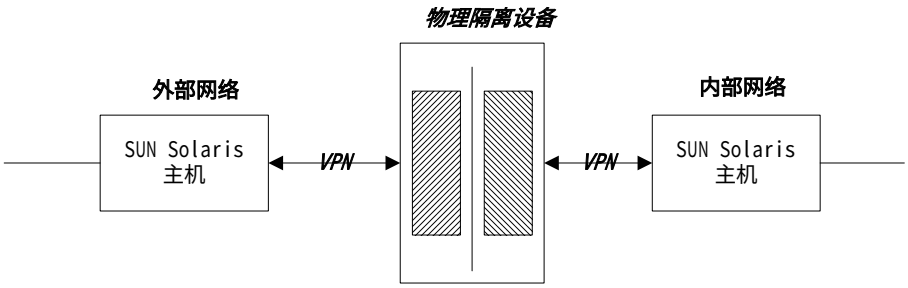
物理隔离系统通常包含电源供应、存储库和在一段时间内只可以一个端口的高速交换机。当外部服务器在硬件设备上装载应用程序级信息后，物理隔离系统中的交换机与外部系统切断连接，而连接到内部系服务器。

为保证物理隔离系统两方的服务器都宕机情况下系统仍然可以工作，在物理隔离系统和服务器之间需要使用 VPN。

3.4.2 工具

Sun 公司建议物理隔离系统采用国内公司的第三方产品。

3.4.3 咨询流程



基于图示意的物理隔离设备网络连接方式，Sun 提供的物理隔离系统的咨询服务包括以下工作：

1．检查网络结构设计，包括物理隔离设备在网络中的位置

2．部署并进行与物理隔离系统相连接的 Sun 系统的 VPN 的基本测试

3.5 入侵检测

3.5.1 内容提纲

使用入侵检测软件通过自动检测网络数据流中潜在入侵，攻击和滥用方式。同时深入了解系统整体安全性以及遵守的策略以及网络内部的运行情况。

Sun 建议采用第三方产品进行入侵检测，由第三方厂商或代理商安装、配置并测试入侵检测软件，并编制相应的文档。Sun 提供咨询服务，建立入侵检测策略，并审查入侵检测的有效性。

3.5.2 工具

使用铁道部已有的入侵检测软件系统。

3.5.3 咨询流程

入侵检测系统的咨询服务包括以下工作：

1. 制定入侵检测策略，管理流程；一些入侵检测基本策略和管理规程提纲如下：

   - 入侵检测应该实时连续进行，并建立全面的攻击方式库；
   - 字匹配扫描：定义表明可能会违反策略的字方式。这种方式可以防止了未经授权就通过 e-mail 或 Web 发送敏感数据等情况的发生；
   - 网络使用日志：网络管理员跟踪最终用户、应用程序等的网络使用情况。它有助于改进网络策略规划；
   - 远程管理：远程用户可以通过 TCP/IP 或调制解调器连接访问运行入侵检测软件的工作站，按照入侵检测软件管理员定义的许可内容，查看和监视入侵检测

数据、修改规则和生成报告；

- 入侵日志及分析：应指定日志归档地点，在档案中记录会话的规则。然后通过浏览器过滤、排序和查看归档信息，并创建详细的报告。

2. 制定入侵检测系统的部署和测试方案并撰写操作手册；

3. 部署和测试入侵检测系统。

3.6 完整性保证

3.6.1 内容提纲

黑客常用的一种攻击方法是 root kit，它包括一些取代当前系统管理功效的程序，阻止系统操作人员发现系统已经入侵。例如，有一个 Unix 程序叫做 ps，可以显示所系统中运行的所有进程。当黑客控制了系统后，他首先可以设计一些特洛伊木马程序或者 daemon 运行在系统后端，但这些程序的进程可以通过 ps 命令显示出来。为避免这种情况，黑客替换 ps 命令，使之不能显示特洛伊木马或者 daemon 进程，而可以显示其它所有的进程。

一般说来，路由器、交换机和防火墙的配置对整个网络安全来讲是关键的。不期望的配置文件的变动可能是系统遭到侵入的标志，也是潜在危险的信号。可能会引起安全事故。同时配置文件的不受控变化也使管理员不容易解决有关问题。

作为中长期的网络安全建设目标，铁道部需要建立完整性保证机制。完整性保证工具可以监控网络中的关键资源的任何变化。可以监控系统中配置文件、系统文件和数据文件的变化。此外，由于完整性保证工具了解系统的变化，对于被入侵的系统，可以通过恢复单独的文件和资源而快速恢复系统，而不必重构整个系统。

3.7 病毒防范

3.7.1 内容提纲

病毒检测服务器能扫描电子邮件消息(SMTP)、网页内容(HTTP)和文件内容(FTP)，检测和清除其所携带的病毒。

3.7.2 工具

Sun 推荐第三方产品方案，所选择的软件应具有全面的病毒查杀功能，包括可执行文件、压缩文件、电子邮件、Office 文档、HTML 文档等多种文件类型内部的病毒。工具可以集检测、清除、治愈为一体，形成全面的反病毒机制。

3.7.3 咨询流程

病毒扫描产品的咨询服务包括以下工作：

1．建立病毒防范规程和处理流程。下面是一个基本内容的示例提纲：

- 使用全公司统一的，可以获得技术支持的防病毒软件；
- 对可疑的不明来源的邮件的附件或宏文件的处理规程；
- 下载文件的规定；
- 直接的磁盘读/写共享的规定；
- 使用软盘的规程；
- 关键的数据和系统配置的备份和存储规定；
- 特定的运行状态和防病毒软件冲突的处理方式；
- 定期进行防病毒的检查。

2．制定病毒扫描产品的部署和测试方案并撰写操作手册；

3．部署和测试病毒扫描产品。

3.8 内容过滤

3.8.1 内容提纲

作为中长期的网络安全建设目标，铁道部需要建立内容过滤机制。内容过滤阻止铁道部用户去浏览 Internet 上的限制级内容。通常情况下，阻止用户通过电子邮件或 FTP 方式将敏感信息发送到 Internet 上。

内容过滤应该使用多种过滤方法。这些方法包括 URL 与域过滤、内容短语过滤、PICS 过滤、MIME 过滤、文件扩展过滤、 POST 限制等。内容短语过滤那些包含不适宜语句的内容；POST 过滤可以限制或锁定 Web 上传。URL 与域过滤能处理大量列表。

3.9 关键服务器系统的安全咨询

3.9.1 内容提纲

为了增强铁道部关键业务服务器的安全，Sun 建议在 Web 服务器、DNS 服务器、代理服务器、目录服务器上提供下列客户化的咨询服务：

1. 简化操作环境；
2. 确定操作系统补丁并及时更新
3. 追踪、侦测上述铁道部关键业务服务器的安全漏洞
4. Solaris 操作系统安全性固化

Sun 将审查和分析业务、技术和应用需求以建立配置规范，并遵循 Sun 的最佳实践实施这个配置。在 Solaris 操作系统安全性固化实施中培训铁道部的员工相关知识和技能。

3.9.2 工具

推荐使用 Sun 专业的 Solaris 安全性工具包 JASS（JumpStart[tm] Architecture and Security Scripts）。JASS 提供灵活的可扩展的机制最小化、固化和保护 Solaris 操作环境，使 Solaris 系统的安全防护自动化处理。Sun 公司推荐定期追踪系统的安全漏洞。

JASS 以尽可能小的对主机系统的更动获得最大的作用，不依赖于主机使用的目的，可以在每个系统上运行多次。

JASS 的基本功能特性包括：

1. 支持绝大多数 Solaris OE 安全特性，预定义了 74 个固化功能和 14 个文件模板；
2. 模块化和灵活的结构；
3. 集成了直接文件复制功能；
4. 高可配置性，使用变量来制定大多数特定内容；
5. 有助于实施系统安全策略，包括初始固化,补丁/生命期管理
6. 已经完成的 74 个功能包括如下几个方面：
   - 禁止功能，禁止一些功能和服务；如 Apache 服务；
   - 使能功能，使能一些功能和服务；如栈保护功能；
   - 安装功能，安装特定部件，如安装 sulog；
   - 最小化功能，如最小化 iPlanetWS;
   - 打印功能，如打印 jumpstart-environment；
   - 移去功能，如移去 unneeded-accounts；
   - 设置功能，如设置 user-password-reqs；
   - 更新功能，如更新 cron-log-size。

JASS 可以方便的进行客户化，使用了 40 多个动态和静态变量配置 JASS，以适应铁道部的安全策略要求和应用要求。

3.9.3 咨询流程

此部分咨询服务包括以下工作：

1. 定义流程和步骤，以确保 Solaris 操作系统补丁得到及时更新
2. 定义流程和步骤，以便追踪和侦测铁道部关键业务服务器的安全漏洞
3. 固化 Solaris 操作系统，简化操作环境

   固化Solaris操作系统的咨询服务流程如下：

   1） 审查当前服务器配置

   2） 与铁道部IT员工访谈，获取安全性需求，包括：

   - 访问控制
   - 认证和授权
   - 保密

   3） 获取服务器上应用和服务的需求和使用方式

   4） 设计操作系统构造规范，包括建议的规程和处理

   5） 为构造规范提供配置信息和文档变更

   6） 按照构造规范实施服务器

   7） 测试服务器实施

4. **提交 Solaris 安全性工具包 JASS 的源程序和相关文件，**传授相关知识。

3.10紧急响应体系

3.10.1 内容提纲

虽然我们为铁道部采取了各种安全措施，减少系统的安全隐患，仍然可能会发生内部或外部的安全问题。Sun 认为应建立紧急事件响应体系，万一紧急事件发生了，可以增强铁道部的应急响应能力和应急响应流程。

3.10.2 工具

在紧急响应体系中不需要工具。

3.10.3 咨询流程

此部分咨询服务包括以下工作：

1. 确定铁道部关键资产和关键风险

Sun 公司将与铁道部一起，确定有价值的和机密的关键数据，明确何种事件可能损害铁道部的关键资产，以及这些事件如何会发生。

2. 建立事件响应计划建议书

通过至多 3 次的访谈，并基于最佳实践，提交安全事件响应计划建议书，并在必要时举行 1 次研讨会。建议书的主要内容示例如下：

- 定义事件发生时的处理步骤
- 如何检测事件，如何确认安全事件
- 决定是否需要起诉

- 事件发生后需要首先完成的工作
- 建立事件响应队伍，定义队伍的责任和分工
- 如何恢复到事件发生前的状态
- 需要保留什么证物，如何保留证物
- 确定事件的紧急程度
- 评估已遭破坏数据的价值

3.11 日志系统与审计

3.11.1 内容提纲

Sun 公司建议铁道部应设立一个审计追踪日志系统，审计服务器、防火墙和各种安全组件，同时建立日志管理策略。

3.11.2 工具

Sun 建议采用第三方厂商的日志分析和审计产品。

3.11.3 咨询流程

日志分析和审计的咨询服务包括以下工作：

1．建立日志分析和审计策略，策略的一些内容提纲如下：

- 日志分析和审计系统的部署；
- 日志分析和审计的查询、统计和报表规定；
- 日志分析和审计系统备份策略；

- 日志分析和审计文件的存储和备份策略；
- 日志检测的阈值设定，及相应处理规则；
- 日志警告的通知方式，7×24 小时的响应流程；
- 日志的分级分类；如调试信息、消息、警告、错误、严重错误；负载日志、事件日志、自我日志等。

2．审查日志分析和审计系统的管理策略符合性

3.12 安全策略

3.12.1 内容提纲

在安全策略咨询服务中，Sun 将提供铁道部员工建立安全策略的流程培训，并开发安全策略建议书。在咨询服务中，Sun 将和铁道部员工一起评估铁道部处理和运行环境，铁道部对安全性的期望，现有法律法规，契约和必须遵守的限制，已有的安全文档、流程、规程和当前及计划中的安全系统。Sun 将分析这些信息，并确定铁道部的安全需求，基于此开发符合铁道部特定需求的安全策略建议书。

咨询服务由知识传递，获得相关信息，安全策略建议书开发，提交安全策略建议书等内容构成。安全策略建议书将覆盖的基本领域包括：

- 信息管理
- 系统运行
- 系统完整性和控制
- 网络和通信
- 应用开发
- 入侵检测和事件处理
- 审计和监控
- 备份、储存和恢复

3.12.2 咨询流程

安全策略的咨询服务包括以下工作：

1. 举行安全策略研讨会，向铁道部员工传授安全策略开发方法和流程；
2. 基于与关键人员至多 3 次的访谈，收集、分析、评估现有安全策略、安全需求及相关信息，包括：应用、系统和网络间的数据流以及信任和控制点；铁道部环境整体保密性、完整性、认证、授权、责任、可用性及保护级别的需求；确定适用铁道部的安全策略部件，其目标、边界、适用性和非适用性；目前安全性设施和加密设施的实施情况；关于信息备份、装入、存档、介质管理、储存、恢复的情况；入侵检测需求和事件处理等；
3. 建立基于上述需求信息的安全策略建议书；
4. 通过研讨会向铁道部提交安全策略建议书。

下面的安全策略建议书主要内容框架是一个示例：

- 数据的责任人、分类和安全性
- 数据和资源访问
- 口令使用
- 加密的使用和密码管理
- 网络安全性
- 电子邮件的责任人、使用和运行安全要求
- 安全事件报告流程
- 安全事件响应流程
- 监控和审计
- 防火墙实施和管理
- 病毒预防和保护
- 终端用户责任和被认可的使用方式
- 记录的储存和备份
- 安全条例和教育

- 变更控制和配置管理

3.13安全流程

调查显示 IT 行业中 30%的安全失败都源于不安全的流程。基于上述安全策略建议书，Sun 公司的经验和最佳实践，以及铁道部的具体情况，我们在以下方面完善安全流程：

1. 固化操作系统
2. 远程管理
3. Telnet 和 Ftp
4. 主权限
5. 远程访问和远程执行
6. 基于主机的 TCP 访问控制
7. 审核检查
8. 网络文件系统
9. X Window 系统
10. 防火墙访问控制和配置、更改
11. Web 服务器
12. 邮件服务器
13. 域名服务器
14. Cisco 路由器
15. 日志管理
16. 服务器备份、恢复
17. 配置管理

18. 漏洞扫描

3.14 系统的可扩展性

随着铁道部网络负荷的增长，可以通过水平和垂直方面增加其扩展性。对于用多进程或者多线程技术实现的工具，Sun 公司的软件和硬件平台可以提供完全的二进制兼容，从单 CPU SPARC 到近百个 CPU 的扩容等。对于基于硬件的产品如物理隔离设备，铁道部可以通过在同一级别上增加更多的产品来适应更大的负荷。

3.15 培训

铁道部系统管理员、网络管理员和安全管理员得到正规、有效的培训，对于铁道部系统的维护是非常重要的。Sun 公司在 Solaris 管理和网络管理上拥有一个完整的培训程序，覆盖了如何安全管理系统和网络等方面。第三方产品供应商也应对其产品的系统管理方面提供培训。Sun 强烈推荐铁道部应确保对系统管理员的正规培训。

在安全咨询服务项目中，采用培训、实验、研讨会、工作中培训等方式进行相关的知识传递。详见关于培训的章节。

4 应用级安全架构

铁道部现存众多的业务系统，需要采取安全有效的方式进行应用系统的集成。本章分三节介绍我们提出的应用程序安全架构。首先我们对铁道部现存的状况进行分析，提出实施的目标及采取的一般性策略。在第二节我们介绍针对铁道部的需求而提出的解决方案，包括认证体系、单点登陆(SSO，Single Sign On)、原有系统的改造和目录服务的部署等。最后一节我们描述了支持该方案的各个软件产品架构及其主要功能。

4.1 目标及其分析

铁道部的目标是建立一个集中式的应用程序认证与授权机制，统一管理用户对应用程序的合法访问。建立统一的企业信息入口，建立统一的用户管理机制，实现基于 PKI 的单点登陆功能（以下简称 SSO）为用户提供方便性和有效性。

本节首先分析了铁道部应用程序的现存状况及其迫切要求，而后依据 Sun 公司在大量应用中总结出的系统方法论提出了总体的目标及实现途径。

4.1.1 现状

铁道部现存众多的业务系统，可能包括基于 Web 的应用系统和基于 C/S 结构的应用系统。

这些应用系统处在孤岛状态，彼此之间缺乏联系。应用系统都拥有各自的用户管理、认证和授权功能，造成资源的浪费和效率的低下。可能的状况见下图：

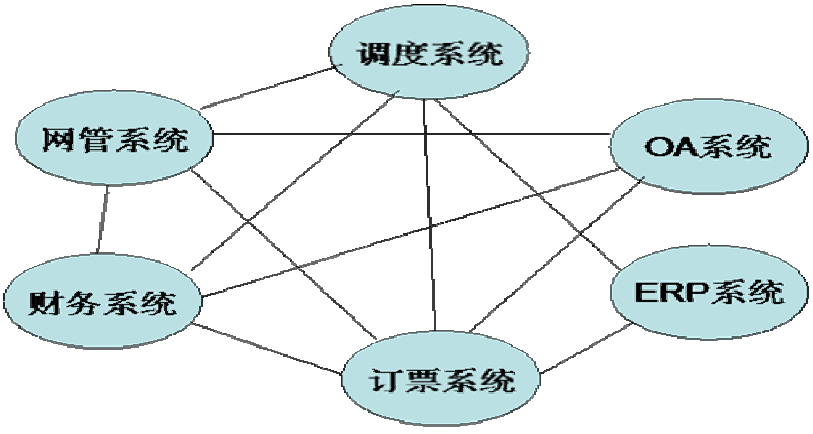


图 1、业务系统的蜘蛛网

这种状况造成的弊端是：

- 信息孤岛或无规则交叉

- 管理复杂，浪费资源
- 效率低下
- 没有统一的用户管理和权限管理，缺乏安全管理

考虑到目前的状况和将来的发展，铁道部内外部应用系统的用户包括客户、供应商、员工和合作伙伴等。而目前使用的应用程序却拥有各自分散的用户认证、授权和权限分配功能，类似于下图：

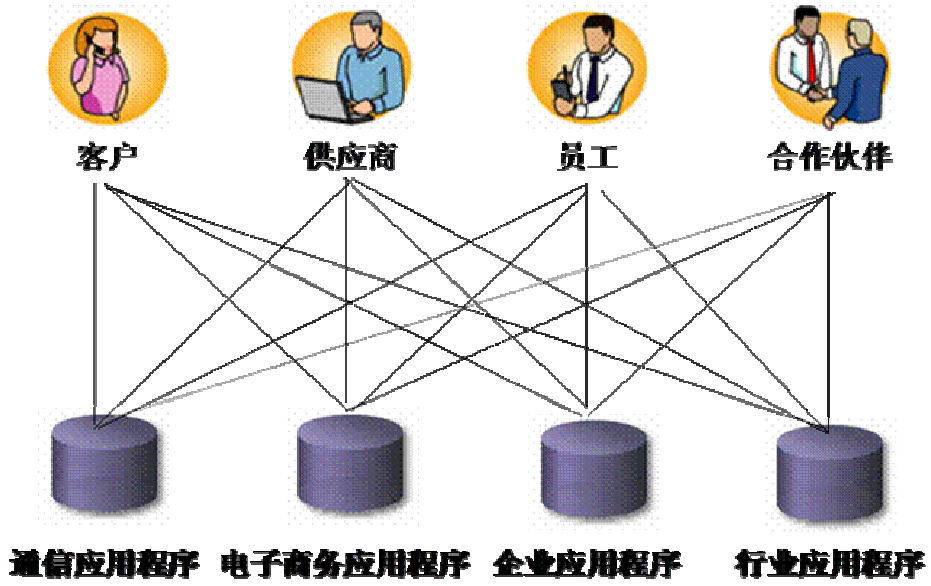


图 2、分散的用户认证授权管理

造成的后果是：

- 用户难以维护，没有统一的视图了解用户对各个应用系统的访问权限和访问记录；
- 增加一个新用户将花费相当长的时间，因为每增加一个用户都可能需要添加到每个应用系统中；
- 对于离职员工，需要花费大量的时间从应用系统中逐个删除该用户，导致非常大的安全隐患；
- 随着企业规模的扩展，带来的用户管理费用将是惊人的

因此，迫切需要构建一个基础架构，来统一管理各类用户对应用系统的安全访问。

4.1.2 参考的方法论

Sun 公司在项目分析、设计和实施各个阶段都运用了业界先进的方法论作为行动的指导，保证工作的规范性和有效性。

分析阶段的四层架构图

Sun 公司以四个层面的架构描述复杂的系统状况，即客户端层(Client Tier)、表现层(Presentation Tier)，业务层(Business Tier)和资源层(Resource Tier)，可参见下图。

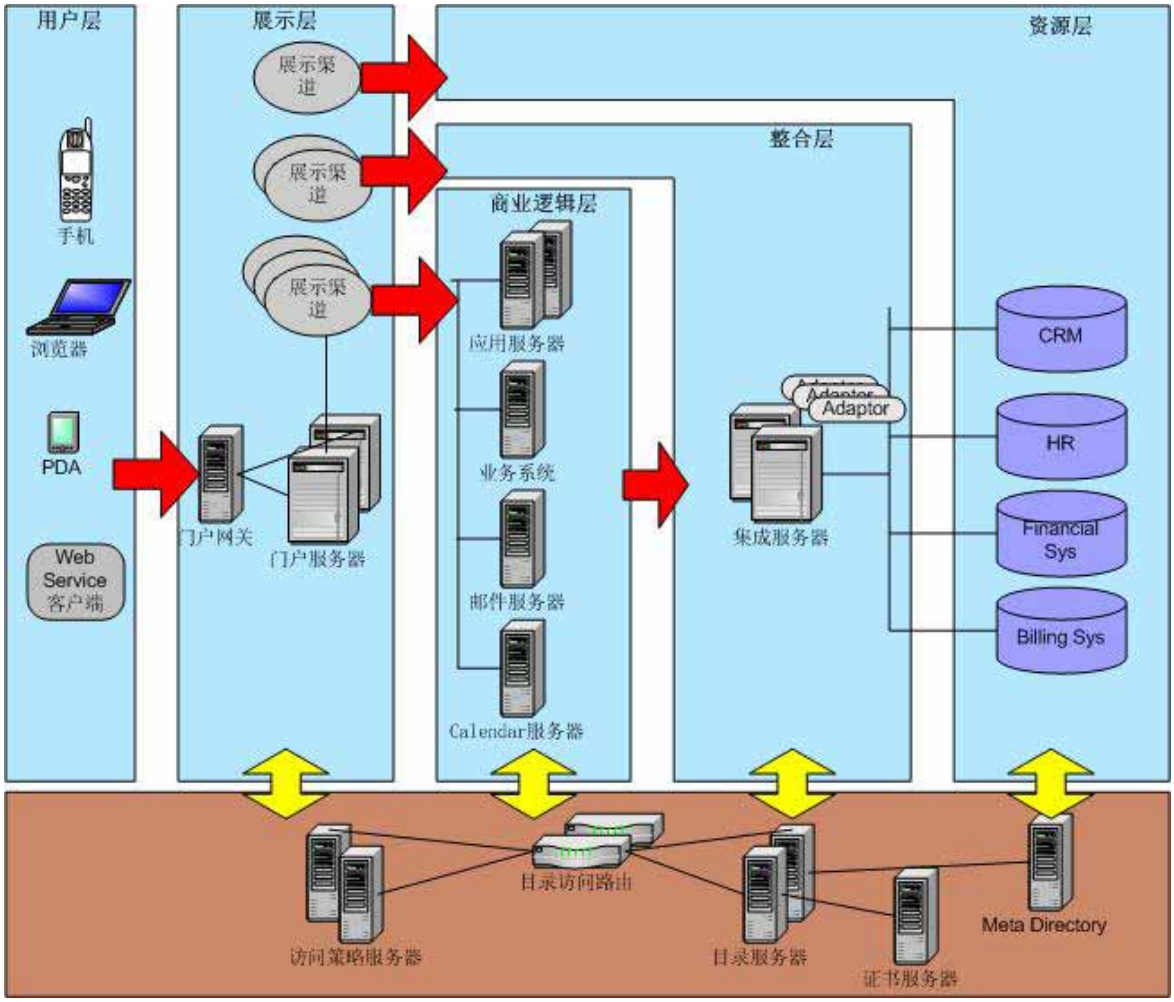


图 3、Sun 的复杂系统方法论

客户端层包括各种信息存取方式，如浏览器、PDA 等。基于实际需要，集成可能在其中多个层面展开。表现层包括网关和门户系统，通过各个频道访问业务层的数据。业务层包括各种实际业务系统，如基于 Domino 或 Oracle 的应用系统。资源层即各种信息库，如 DB、ERP 系统等。在不同的层面，可能与认证服务器、策略服务器等交互。

根据铁道部的现存应用系统的状况，应该是：

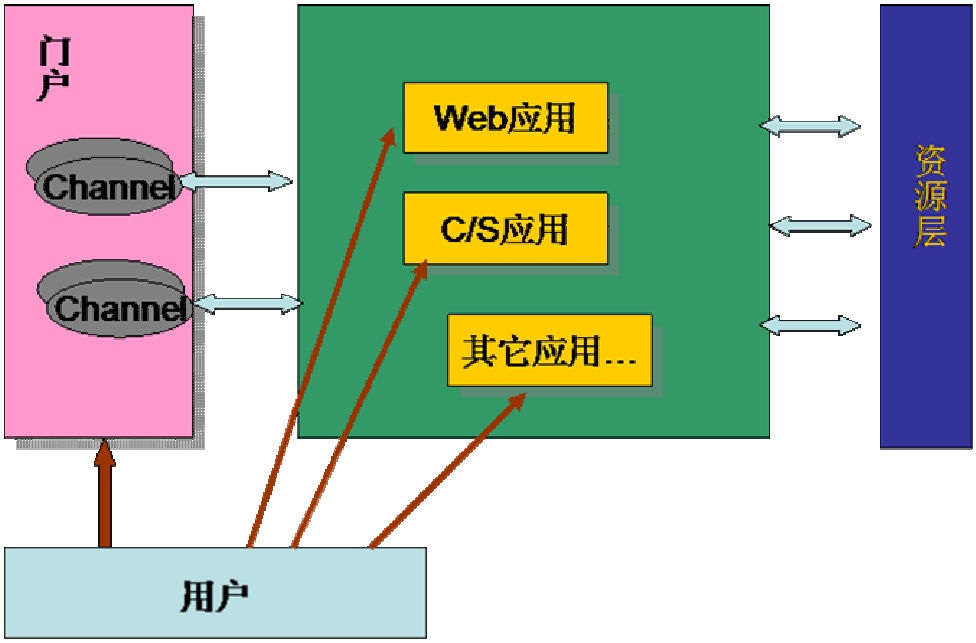


图 4、铁道部的应用发展状况

软件设计阶段的 RUP 方法论

Sun 在设计软件时所采用的方法是 Rational 统一过程(RUP)。RUP 的特性包括：迭代过程、控制过程、重视模型、注重软件体系结构、受使用案例推动、采用面向对象技术、基于组件的软件开发、可配置过程、持续质量控制、工具支持等。

RUP 以以下两个尺度展开：

1. 依照核心工作流，即按照性质对活动进行逻辑分组

2. 依照时间，即过程展开时的过程生命周期方面

过程是按时间（阶段）和内容（核心工作流）进行组织的。第一个尺度代表过程的静态方面：如何按核心工作流、活动等描述过程。第二个尺度代表过程的动态方面，因为过程是按照周期、阶段、迭代和里程碑进行制定和表示的。

RUP 将一个开发周期分为初始、细化、构建和交付四个连续的阶段。每个阶段以一个良好定义的里程碑为结果。该里程碑是一个时间点，在这个时间点必须作出某些重要决定并因此而必须实现了关键目标。

系统设计阶段的 SunTone 方法论

SunTone 体系结构方法论是 Sun 将 Sun ONE 的理念运用于企业的方法，是一整套从设计开发到交付 Web 服务的实践指南。

SunTone 体系结构将以下三个重要方面结合在一起，建造坚实的解决方案：

- 逻辑拓扑，也叫分层，分层包括客户层、表示层、商业逻辑层、数据集成层,和资源层。定义分层是为了支持多种渠道的接入，使之具有一定程度的安全性和可扩展性。
- 技术级别的区分与说明：把不同类型的工具区分开来，并标明各级别之间的标准接口。这样做是为了避免各级技术的依赖关系过于紧密，以至影响到将来选择的自由度。
- 系统的功能：包括用户级(可用性，可存取性)、服务级(性能，可靠性，可用性)、策略级(可扩展性，灵活性)、系统级(安全性，可管理性，可维护性)。尽早决定一个解决方案的系统质量要求(服务质量 Quality of Service)是非常重要的。

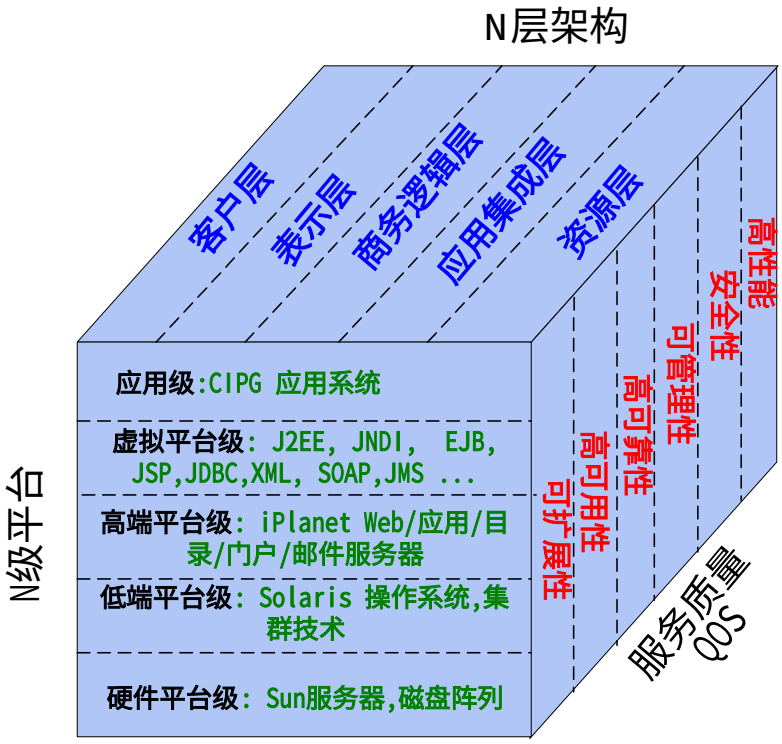


图 5、SunTone 示意图

我们将系统描述进一步组织成一套体系结构窗口，每个窗口表示从某一个方面所看到的系统功能的子集。系统分级则包含了许多窗口，对分级的定义是这样的：

- 应用级包含特定应用的组成部分，通常大部分是特别编制的代码；
- 虚拟平台级将应用与高级平台级的具体实现区分开来，使应用与平台供应商无关，例如 J2EE 就是一个这种概念的例子；
- 高端平台级包括象 Web 服务器，应用服务器及各种中间件产品；
- 低端平台级由操作系统环境和与之相关的低层系统服务构成；
- 硬件平台级包括物理的运算处理结点和网络连接

整体的系统质量窗口将所有分层和分级结合在一起。它对于每一个质量要求定义出所需的产品和技术，描述在该体系结构下系统质量的目标是如何达到的。

4.1.3 目标需求

依据对铁道部现状的分析并参考系统方法论，我们认为铁道部应用程序安全架构的设计应设定以下主要目标：

- 实现用户统一的身份管理
- 在应用系统之间实现 SSO
- 实现应用系统内容的集中展现
- 实现高可用性、扩展性和可管理性，提供负载均衡，保证无单点失败

统一的用户身份管理

为了应用系统安全、集中的管理，必然需要建立用户身份的统一管理机制，实现：

- 一致性的网络安全策略
- 集中管理的认证和授权机制
- 完整的身份活动周期管理

统一的身份管理提供一站式的

- 身份
- 管理
- 访问控制/执行
- 单点登陆

统一身份管理的好处在于：

– 增强安全性

- 集中式的策略管理，实现单点访问控制
- 通过数字证书、令牌卡、智能卡等手段增强应用程序和资源的安全性

– 减少费用

- SSO 保护 IT 投资，提高用户效率
- 集中式的用户、策略和服务管理

– 增强运行效率

- 对各种服务而言，一点即可实现创建、维护和删除用户帐号等各种功能
- 在各种数据源之间保持信息同步，如 Windows 帐号、邮件帐号和人力资源系统等

实现 SSO（单点登陆）

应用程序的安全性意味着按用户的安全属性，在应用程序上给用户分配其相应的访问权限。无论用户处于怎样的位置，使用怎样的设备，都可以有效地访问这些应用程序，这对许多企业而言是非常重要的。实现用户一次登陆就可以获得对多个应用程序的访问能力，在提高效率方面扮演着重要角色。在美国的研究表明，用户因为使用多帐号和多口令的麻烦，造成每年 44 个小时的浪费。同时，多点登陆也引起口令遭破坏的风险。

然而从安全的角度我们也应看到事物的双面性，SSO 的实现也消除了许多非法用户成功入侵后的许多障碍。完成 SSO 后，入侵者在成功表现出合法用户的身份后，就可以顺利访问对该用户授权的所有网络资源和应用系统。因此对 SSO 部署需要对安全策略和高风险的资产进行完整彻底的评估，这将需要更强有力的认证方法，如硬件 Token、智能卡等。对特别敏感的系统，应考虑一个附加的安全层，如内部防火墙或二级认证系统等。我们建议铁道部应用系统的认证部署一个通用性的 PKI 系统来实现较强的身份认证。

我们建议采用 Sun ONE Identity Server 及其提供的 SDK 和 API 作为实现 SSO 功能的基本框架。具体参见下面的相关内容。

门户系统

门户系统做为企业信息的集中访问的入口。用户可以通过门户的各个频道(Channel)访问集成化了的各个应用系统，极大增强了应用系统的使用率，提高了用户的使用方便性。

用户也可以直接访问业务系统，但与先前使用方式最大的不同之处在于，用户管理、认证和授权等功能已进行了统一的规划和管理。

因此铁道部需要强大、稳定、高性能的门户软件产品。Sun 公司可提供业界领先的门户产品 Sun ONE Portal Server，能充分满足铁道部应用程序集成的需要，具体内容参见下面相关章节。

4.2 方案描述

我们为铁道部设计的应用程序安全架构的部署图如下：

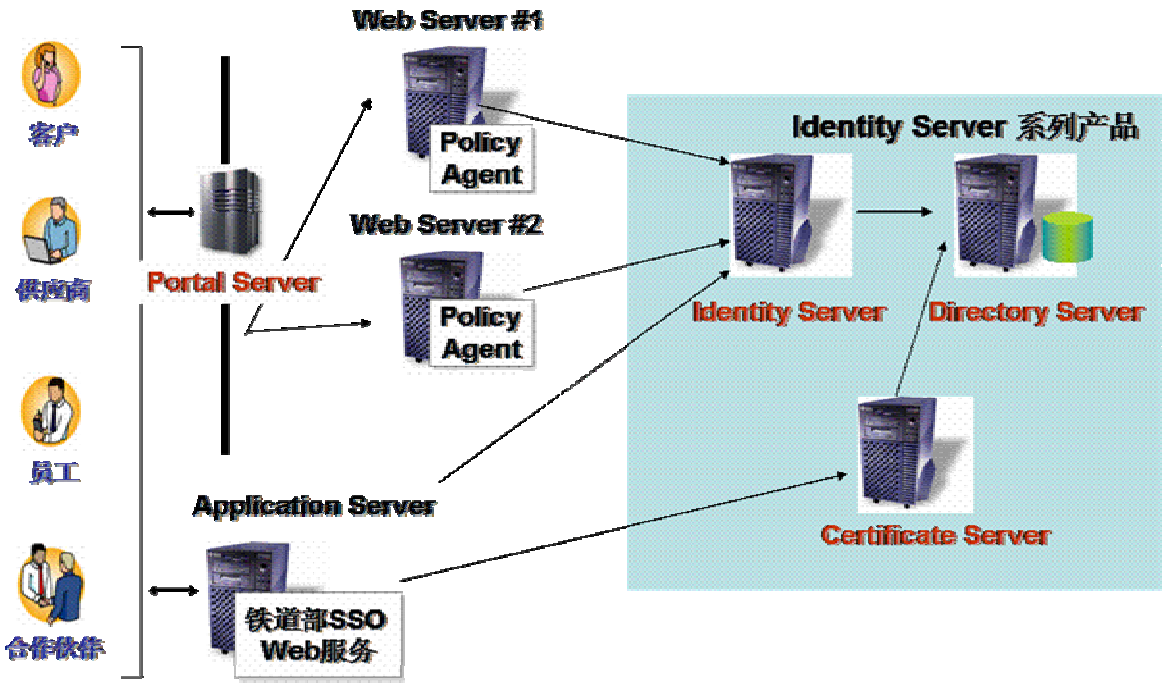


图 6、应用程序架构总体示意图

铁道部应用程序安全架构建立在标准化、集成化的 Sun ONE 身份和访问管理方案之上，包括目录服务、证书管理服务、PKI 认证、访问和策略管理服务等。为进一步了解 Sun ONE 产品，请参看附件 A。我们的目标是为铁道部提供基于扩展性、可靠性和可管

理性的方案，从而获得最高效的服务。我们提供的所有组件均可实现良好的负载均衡并确保无单点失败。

LDAP Directory Server 是方案的基石，提供用户的名称、属性及权限的集中存储器。用户权限包括用户使用应用程序的许可策略。在 Directory Server 之上，Identity Server 是方案另一个重要的组成部分。Identity server 提供认证服务，它包括基于证书的认证和策略服务。Directory Server 与 Identity Server 的策略服务一起，为许多应用程序提供策略执行服务。证书管理系统提供证书管理服务，如向员工或合作伙伴发放和撤销证书等。

门户服务器作为铁道部应用集成系统的表现层，开发的 SSO 组件和现存应用程序等做为业务层，Identity Server 产品系列实现系统的认证体系。

用户通过通过门户的各个频道(Channel)访问集成化了的各个应用系统。对于 Web 应用程序而言，需要在每个应用程序的 Web 服务器上配置 Policy Agent。通过这些 Agent 与 Identity Server 及 Directory Server 进行交互，实现 SSO。

对于铁道部存在的大量 C/S 应用程序，我们将在 Application Server 上开发一个专用的 SSO Web 服务程序实现 SSO。

铁道部应用程序安全框架构的组件关系示意图如下：

- Web 应用程序和 C/S 应用程序使用 PKI 证书进行认证
- 基于 LDAP 目录协议的的统一用户管理系统
- 门户服务器提供内容聚集和 Web 应用程序之间的 SSO
- 证书管理系统发放和管理证书
- 策略服务管理特定资源的授权权限
- 定制的 SSO Web 服务基于 Identity Server SDK 开发，管理铁道部应用程序之间的 SSO
- **用 Mozilla 开放源代码的 PKI SDK 改造铁道部的应用系统的认证功能**

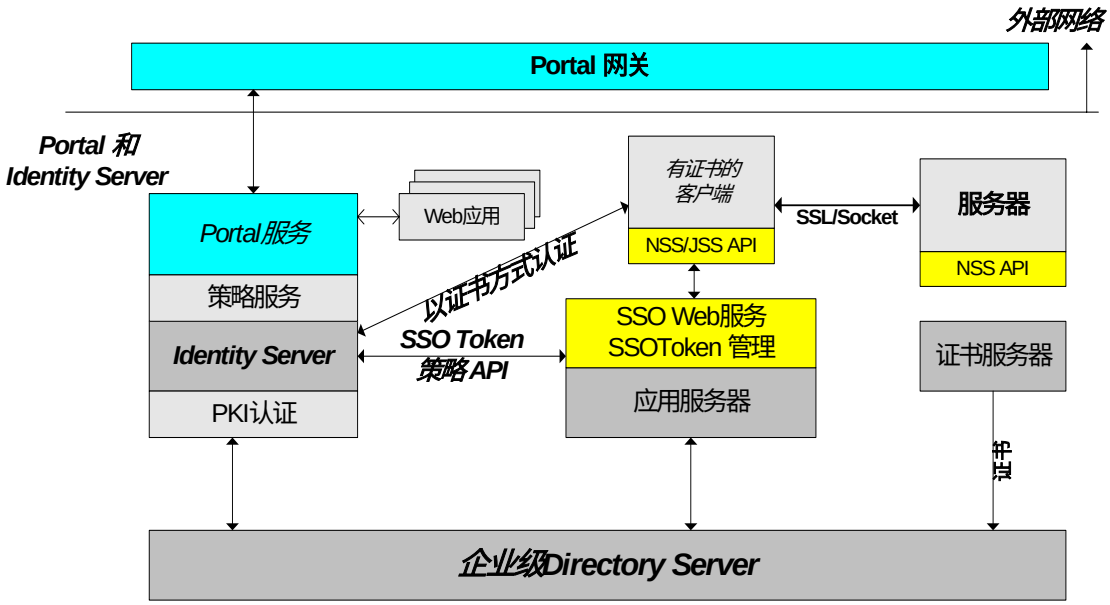


图 7、铁道部应用程序安全框架组件关系

方案的优点在于：

- **经验证的方案架构**。所有方案中推荐使用的组件都经过大量实践的考验。NSS/JSS 广泛应用于 Netscape 浏览器和许多 Sun、Netscape 和 AOL 的产品中。Sun ONE Directory server 和 Identity Server 是行业领先的网络身份管理产品。

- **NSS/JSS 源代码开放**，不仅确保安全性，可以方便地进一步开发。

- **高可靠性和扩展性的方案**。Sun 为铁道部提出的解决方案使用了高可靠性和扩展性的产品，如 Directory Server、证书管理系统和 Web 应用程序框架等。提供的所有组件均满足良好的负载均衡并确保无单点失败。

- **减少了应用程序改造的工作量**。我们使用标准的 XML 和 Web 服务作为访问策略结果的通信方式，因此减少了对现存应用程序的代码改动量。大部分认证代码都可以在源代码开放的 Mozilla 中找到示例，没有必要重新开发，因此提高了开发效率。

考虑到长期规划的目标，铁道部可以使用 Liberty 标准和 SAML 技术获得跨区域的单点登陆功能，如在分路局之间或者与其它外部合作伙伴之间。

目前 Internet已成为团体、个人间主要的交互手段之一。身份是这种其中至关重要的组成部分。现今，Internet上的个体身份信息由不同身份提供者所提供的分散信息组成，如员工信息、Internet门户身份等。这些片断信息是孤立的，高冗余的，联合网络身份是减少这种冗余的关键因素，并为商业运作引入新的模式，在这种新型模式中，用户的身份、个人信息、个性化的在线信息配置等可以由用户自己管理，并通过安全的方式共享给其他组织。一个联合网络身份模型将确保私密性信息只能被合法的组织使用。

Liberty联盟由包括Sun等全球许多著名公司参与，主要目标是共同制定和实行一种身份管理标准，Liberty联盟成员可以在一个跨越不同网络服务提供商和商业机构的网络世界里顺利进行网上交流和交易，而不必担心用户私密身份信息的泄漏。该联盟及其技术构想受到了业界广泛的支持，并迅速成为下阶段IT技术的热点。

有关 Liberty 联盟的详细信息请参见站点http://www.projectliberty.org/

SAML 即 Security Assertion Markup Language，是安全相关信息的交换框架。关于认证和授权的断言以 XML 编码的方式表示，是新的 OASIS 标准。

SAML 确保以最私密的方式共享许可管理数据。当前，集成新的安全特性可能都需要开发很多新的代码，生产和使用安全数据的应用系统之间耦合性过强，SAML 技术可很好地解决这样的问题。SAML 也为跨组织的 Web 应用程序的单点登陆（Single sign-on）功能提供了标准的方式。Liberty 规范基于 SAML。

下图描述了铁道部使用 SAML 和 Liberty 的一种可能的情景。

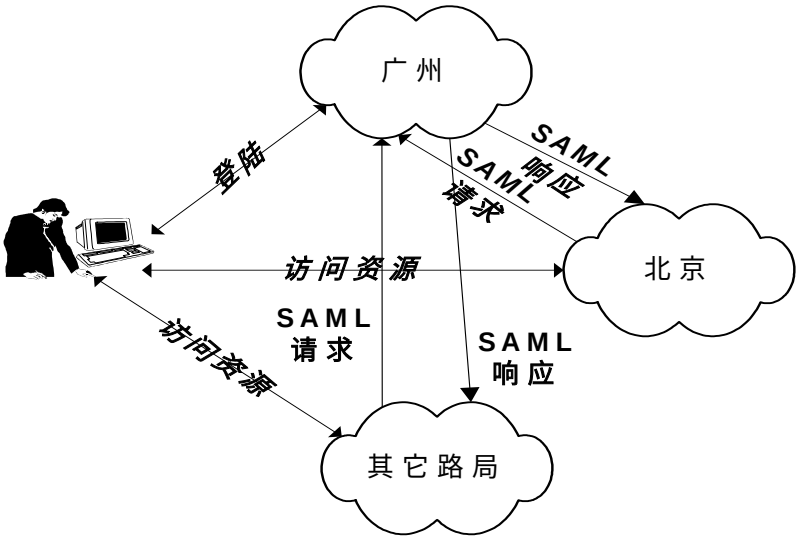


图 8、使用 Liberty 和 SAML 的情景

在图中，用户在登陆到广州站点之后，试图访问北京站点的 Web 资源，支持 Liberty 标准的 Identity Server 将从用户原始登陆地点广州发送一个 SAML 请求，SAML 响应将返回用户登陆信息和 Profile 信息，然后根据用户的 Profile 和策略，评估其访问请求。

方案的更详细内容请参见下面几节。

4.2.1 铁道部基于 PKI 的认证体系

基本的认证方式是采用用户名和口令。在大多数应用程序中，用户名和口令在网络上以明文方式传送，这不具有足够的安全性。公钥加密是更安全的认证方式。

公钥存在于证书中。证书标识了个体、服务器或者其它一些实体。向服务器鉴别一个用户时，客户端对一个随机生成的数据块进行数字签名，并在网络上发送证书和签名数据，如下图所示。可以认为数据的数字签名是客户端提交给服务器的证物。服务器端按照这个证物鉴别用户的身份。

在图中假设用户已经信任服务器并请求访问某个资源。服务器在检查资源的访问控制列表(ACL)的过程中要求客户端进行身份认证。

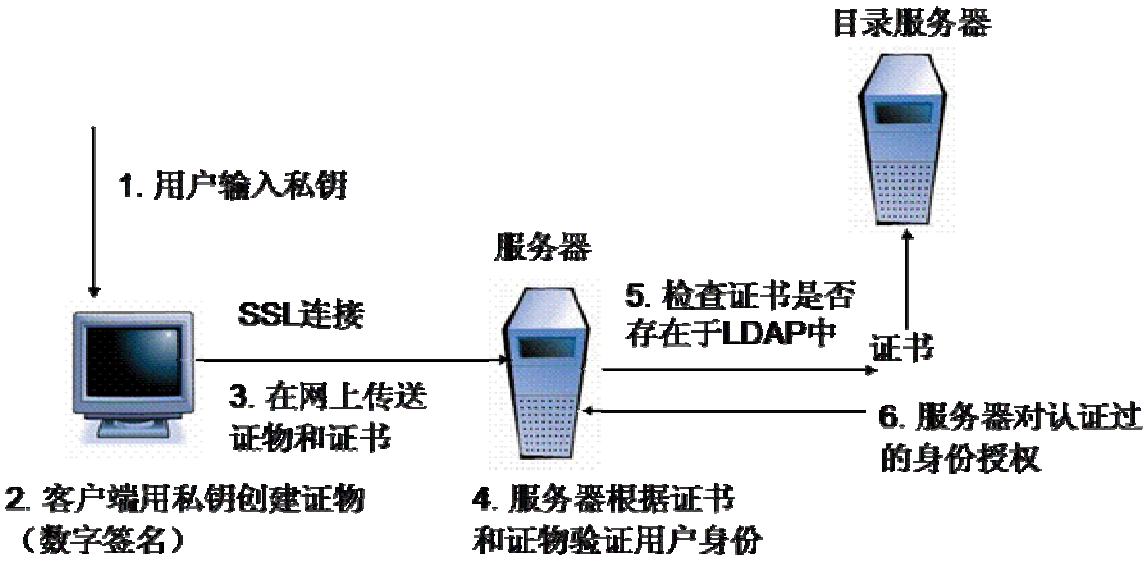


图 9、在客户端和服务器之间使用证书进行认证

不同于基本的认证方式(未经加密的用户名和口令)，上图中描述的过程需要使用 SSL。它假设客户端已经有了一个有效的证书，并可以用它在服务器上鉴别客户的身份。因为该过程基于用户拥有什么(证书)和用户知道什么(保护密钥的口令)，我们称之为“强认证”。

4.2.2 铁道部基于 PKI 的 SSO

SSO 是基于 PKI 方案的基本功能。我们建议的方式是采用一个通用的证书来实现 SSO，而不是对多个服务器需要多个口令进行认证。通用的证书意味着对许多应用程序只需要用一个单独的证书来认证某个用户。

铁道部应用程序环境非常复杂，包括 Web 应用程序和使用 C/C++、Java 或者其它语言开发的的多种 C/S 应用程序。SSO 方案建立在 Sun ONE Identity Server 框架之上，用 PKI 作为主要的认证机制。

应用程序必须能以编程的方式实现读取证书和验证用户等功能，推荐使用 NSS/JSS 或 JDK 开发工具包，它们可以从http://www.mozilla.org 或 www.sun.com 站点上下载。

我们将使用 Sun ONE Identity Server 及其相关 SDK 和 APIs 来构建集中式的认证和授权服务框架。Identity Server 提供集中式的策略服务，Directory Server 作为策略数据和用户数据的存储库。我们也将开发专用的 SSO Web 服务，在 Web 应用程序和铁道部 C/S 应用程序间协调管理 SSO 及策略。

Sun ONE Identity Server 的详细描述参见 4.3 节。

下图描述了铁道部实现 SSO 的框架：

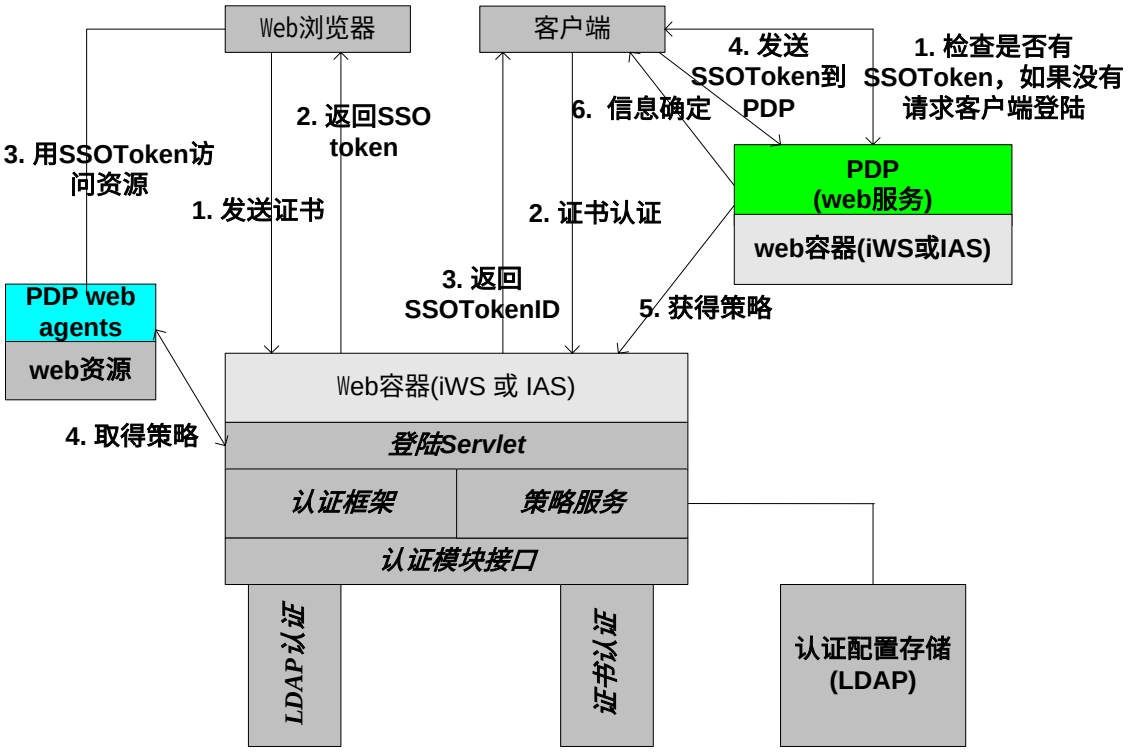


图 10、铁道部 SSO 框架

基于 Sun ONE Identity Server 实现 SSO 方案的原理是共享一个“ SSOTokenID ”的对象。当用户使用支持的认证机制（含证书）向 Identity Server 请求认证时，将产生 SSOToken 作为用户会话，SSOTokenID 将发送回客户端。对于 Web 应用程序，SSOTokenID 以浏览器的 cookie 方式存在。

对于 C/S 应用程序，必须有一种机制在各种应用程序间存储和共享这个 Token。因此需要开发一个专用的基于标准的 Web 服务，在 Identity Server 和应用程序之间实现交互。在 C/S 应用程序情况下，该 Web 服务也担当特定资源的策略结果点(policy decision point)。资源即服务器应用程序本身。专用的 Web 服务将从 Identity Server 中得到相关策略，依据它评估请求并发送给请求者（通常是客户端）相应的结果。依据 Web 服务的指示，如果用户没有存取系统的权限，客户端可能会关闭自己。

策略和用户配置

通过 Identity Server 的管理界面或命令行，给用户指定角色和使用 C/S 程序的相关权限。策略将通过 Identity Server 的控制台配置。

客户端 SSO

客户端应用程序将首先通过 Web 服务检查是否存在 SSOToken，如果存在，说明证书已经通过了 Identity Server 的认证。在这种情况下，不必经过完整的证书验证过程就可以实现 SSO。一旦完成认证，专用 Web 服务将向客户端通知其相应的策略结果。

Web 应用程序的 SSO，主要工作是根据应用程序 Web 服务器的不同，选择不同的 Agent 并进行必要的客户化开发工作，Sun 公司已经提供了许多这方面的商用产品，如针对 WebLogic、Sun ONE Application Server 和 Apache 等 Web 服务器开发的 Agent。

4.2.3 铁道部应用程序的改造

按照铁道部安全的需求，需要对铁道部现存的应用程序进行必要的改造。一些铁道部的应用程序将改造为 PKI 认证方式。如果考虑到客户端和服务器间的数据安全传输，则需要数据加密。

对现存的客户端程序：

1. 读取用户证书和通过 NSS/JSS 库鉴别证书
2. 调用 Web 服务 Agent 确定是否用户已经登陆
3. 如果用户还没有登陆，调用 NSS/JSS SSL 的 API 库向 Identity server 提出认证
4. 从 PDP Web 服务 Agent 中获得策略结果信息，通常采用用 SOAP/HTTP
5. 如果没有授权，关闭应用程序
6. 当成功登陆时，传递 Token 到服务器
7. 清除存在的用户名和口令

对于现存的服务器端程序:

1. 检查 Token，决定是否允许连接
2. 为保证数据的安全连接，可能使用 NSS/JSS 的 SSL API

对于 Web 应用程序，改动将比较少。如果需要将 Web 应用程序配置为一个 Channel，就需要使用相应的 Portal API。

实际改造的集成工作量依赖于许多因素，如开发人员的技能、应用程序的复杂程度和所需要的安全级别等。

NSS 包括详细的 SSL API 文档和示例源程序，阐明了基本的 SSL 功能，如建立加密的会话、服务器端认证和客户端认证等，可以帮助集成过程的起动。如果铁道部还需要复杂的证书管理、智能卡支持或者硬件加速，将增加相应的集成工作量。关于 NSS 参见 4.3 节。

4.2.4 铁道部 LDAP 目录服务的部署

目录服务器集中存储用户身份信息、服务数据、访问策略和证书等。对用户可信性的鉴别过程高度依赖于可信数据存储的性能。Sun ONE Directory Server 是目前存在的最快的 LDAP 数据管理软件，能极大提升整个系统的性能。Sun ONE Directory Server 也提供基础的角色和动态组功能，Sun ONE Identity Server 可以用这些功能管进行身份管理服务，用 Sun ONE Directory Server 集成版展现用户管理的归并视图.

目录系统成功实施的关键在建立高扩展性、可靠性的目录服务器集群，应用程序用它们进行认证（通过 Identity Sever）。Sun ONE Directory Server 提供多主控制器架构，确保不会发生单点失败。

Sun ONE Directory Server 是目前业界最成熟、最可靠和经大量实践验证的 LDAP 目录解决方案，发放了超过 9.5 亿的用户许可证。在许多世界巨型的商业机构中得到广泛应用，如著名的保险公司 AXA、美国美联银行、福特公司、汽车零部件行业的江森自控公司、美国职棒大联盟、摩托罗拉和英国宽带公司 NTL 等。美国前十名财政金融服务公司中的八个都应用了 Sun ONE Directory Server。全球著名的 IT 报纸 eWeek 于 2002 年 11 月 4 日称：“ 最优秀以及最著名的目录服务器是 Sun 公司的 Sun ONE Directory Server 产品 ”。

Sun ONE Directory Server 具有充分考虑高可靠性的功能特征。目录复制技术有助于防止单个服务器失效；事务日志有助于失败后的系统恢复；支持 SNMP 提供灵活的网络管理能力。另外，Sun ONE Directory Server 通过支持在线的备份、配置修改、策划升级和

索引更新等技术，极大减少了由于管理和维护造成的中断和停机时间。

每个服务器可以管理数百万的目录对象和处理每秒数千次的查询，同时目录数据还可以通过逻辑分区分布到多个目录服务器上。在多 CPU 的服务器上，具有线性的性能伸缩能力。允许管理员监视和调整服务器的性能。可以根据实际的使用情况，灵活的建立属性级的索引，对性能进行优化。

我们建议铁道部的每个业务组织在本地网络上都部署一个 LDAP 服务器。本地的 LDAP 服务器是一个 LDAP Consumer 服务器，它复制铁道部整体用户目录的相关内容。这种方式的好处是由于目录服务器部署在用户本地，响应速度足够快，并能减少网络阻塞。

铁道部中心目录服务包括用户记录和用户信任状的主拷贝。为提高可用性需要部署多个主控制服务器。所有的更新将通过 LDAP Proxy Server 路由到某个 LDAP 主控服务器。LDAP Proxy Server 提供对 LDAP Server 的保护和过滤。LDAP 代理也提供负载均衡功能。

如果用户数目很大，可以采用复制 Hub 减轻主控服务器的负荷。主控服务器将复制到 Hub 服务器，而且 Hub 将复制回适当的 Consumer 服务器上，这将减缓主控服务器的负荷。

我们采用多个 LDAP 主控服务器实现 HA（高可用性），因为 LDAP 服务器存储的是企业关键数据，应保证其不间断工作。每个 LDAP 主控服务器可以部署在各个分区域中，如北京、广州、郑州等，利于数据的分流，减轻每个服务器的负荷。

LDAP 部署的复杂性在于如何集成和同步各种存在的本地目录和成员数据库，形成唯一的统一的存储库，这可以通过元目录服务实现。已经存在一些连接器可以帮助映射和连接数据记录。详细的设计在对目前认证机制的评估后完成。

下图是铁道部目录部署的示意图：

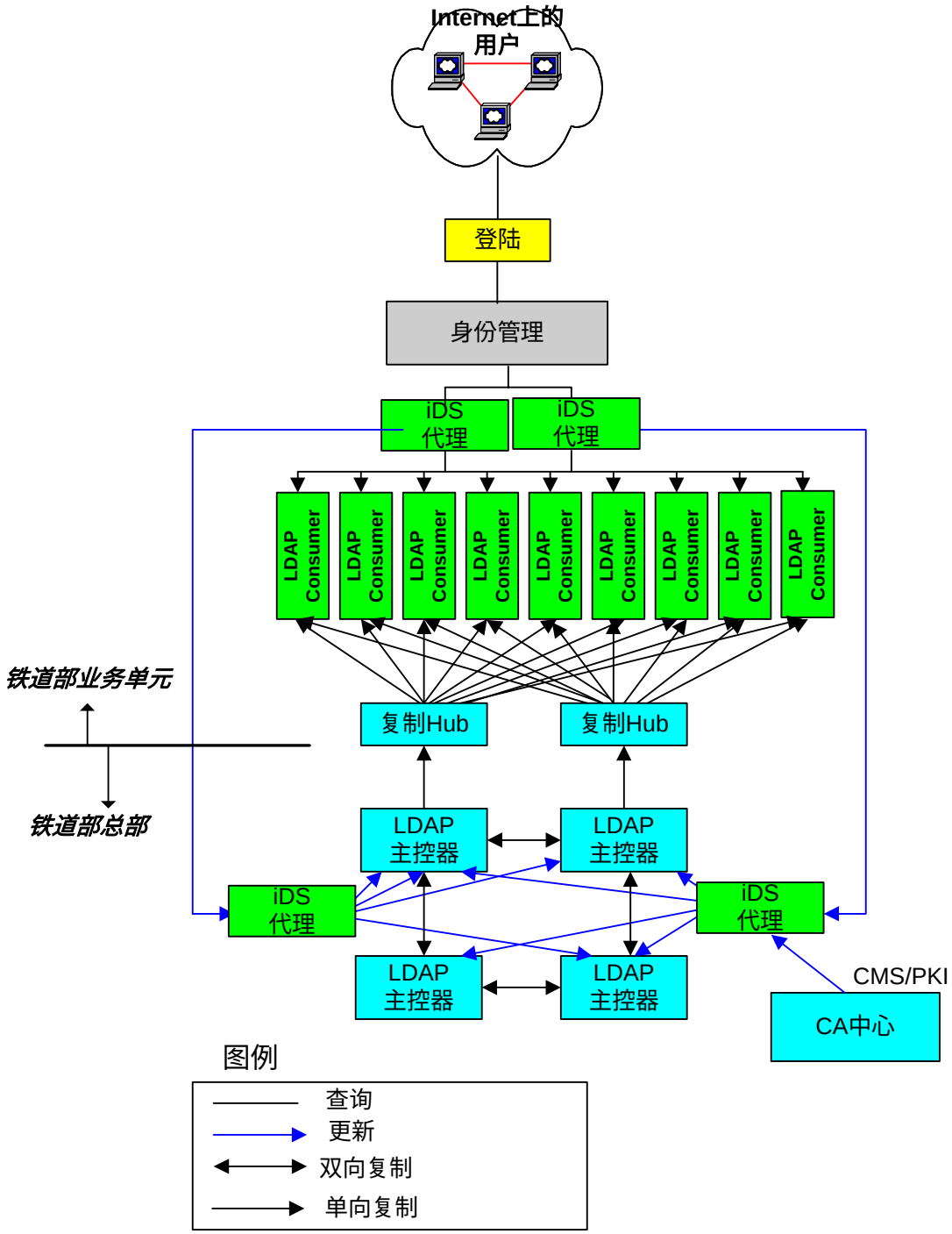


图 11、铁道部目录服务部署图

4.2.5 铁道部证书管理系统

证书是数字证书或电子证书的简称，是网上实体身份的证明。证书由具备权威性、可信任性和公正性的第三方机构签发，因此是权威性的电子文档。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间，发证机关（证书授权中心）的名称，该证书的序列号等信息。

铁道部可以发放标准的 X509 证书。

PKI 组成

典型的 PKI 系统包括证书机构 CA、注册机构 RA、相应的存储库、证书发布系统等。

CA(认证机构)是 PKI 的信任基础，它管理公钥的整个生命周期，其作用包括：发放证书、规定证书的有效期和通过发布证书废除列表（CRL）确保必要时可以废除证书。

RA(注册机构) 提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求，主要完成收集用户信息和确认用户身份的功能。

注册管理一般由独立 RA 来承担。它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。因此，RA 可以设置在直接面对客户的业务部门。对于一个规模较小的 PKI 应用系统来说，可把注册管理的职能由认证中心 CA 来完成，而不设立独立运行的 RA。但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。

PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，可以增强应用系统的安全。

我们建议在各个分局上部署各自独立的 RA 系统，参见图 10。

证书存储库包括 LDAP 目录服务器和普通数据库，用于对用户申请、证书、密钥、CRL 和日志等信息进行存储和管理，并提供一定的查询功能。一般来说，查询的目的有两个：其一是想得到与之通信实体的公钥；其二是要验证通信对方的证书是否已进入“撤销名单”。证书库支持分布式存放，即可以采用数据库镜像技术，将 CA 签发的证书中与

本组织有关的证书和证书撤消列表存放到本地，以提高证书的查询效率，减少向总目录查询的瓶颈。

证书格式

X.509 证书所包含的主要内容如下：

- 证书版本号（Version）：版本号指明 X.509 证书的格式版本，现在的值可以为 0、1、2，也为将来的版本进行了预定义。
- 证书序列号（SerialNumber）：序列号指定由 CA 分配给证书的唯一的数字型标识符。当证书被取消时，实际上是将此证书的序列号放入由 CA 签发的 CRL 中，这也是序列号唯一的原因。
- 签名算法标识符（Signature）：签名算法标识用来指定由 CA 签发证书时所使用的签名算法。算法标识符用来指定 CA 签发证书时所使用的公开密钥算法和 hash 算法，须向国际知名标准组织（如 ISO）注册。
- 签发机构名（Issuer）：此域用来标识签发证书的 CA 的 X.500 DN 名字。包括国家、省市、地区、组织机构、单位部门和通用名。
- 有效期（Validity）：指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。
- 证书用户名（Subject）：指定证书持有者的 X.500 唯一名字。包括国家、省市、地区、组织机构、单位部门和通用名，还可包含 email 地址等个人信息等
- 证书持有者公开密钥信息（subjectPublicKeyInfo）：证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。此标识符包含公开密钥算法和 hash 算法。
- 签发者唯一标识符（Issuer Unique Identifier）：签发者唯一标识符在第 2 版加入证书定义中。此域用在当同一个 X.500 名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500 名字。可选。
- 证书持有者唯一标识符（Subject Unique Identifier）：持有证书者唯一标识符在第 2 版的标准中加入 X.509 证书定义。此域用在当同一个 X.500 名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500 名字。可选。

- 签名值（Issuer's Signature）：证书签发机构对证书上述内容的签名值。

CA 框架模型

一个典型的 CA 系统包括安全服务器、注册机构 RA、CA 服务器、LDAP 目录服务器和数据库服务器等。如下图所示。

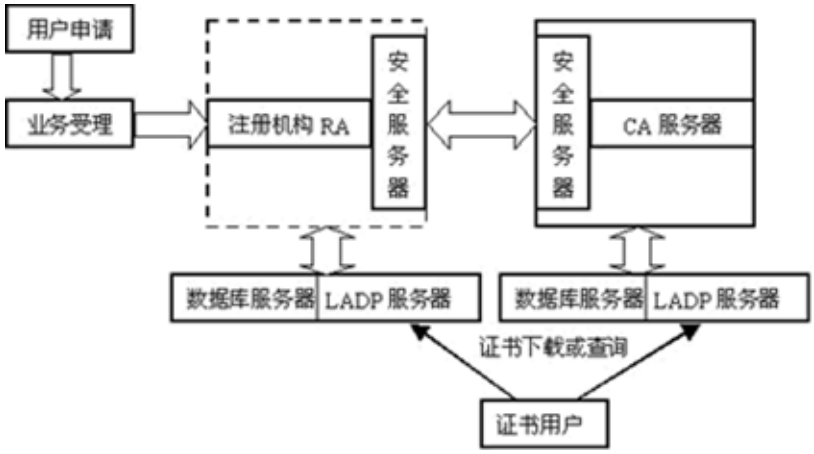


图 12、典型 CA 框架模型

安全服务器：安全服务器提供证书申请、浏览、证书撤消列表以及证书下载等安全服务。用户与服务器之间的所有通信均以安全服务器的密钥进行加密传输，只有安全服务器利用自己的私钥解密才能得到明文，防止其他人通过窃听得到明文，从而保证了证书申请和传输过程中的信息安全性。

CA 服务器：CA 服务器使整个证书机构的核心，负责证书的签发。CA 首先产生自身的私钥和公钥（密钥长度至少为 1024 位），然后生成数字证书，并且将数字证书传输给安全服务器。

注册机构 RA：在 CA 体系结构中起承上启下的作用，一方面向 CA 转发安全服务器传输过来的证书申请请求，另一方面向 LDAP 服务器和安全服务器转发 CA 颁发的数字证书和证书撤消列表。

LDAP 服务器：LDAP 服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入到服务器上。这样其他用户通过访问 LDAP 服务器就能够得

到其他用户的数字证书。

数据库服务器：数据库服务器用于认证机构中数据（如密钥和用户信息等）、日志合统计信息的存储和管理。实际的系统应采用多种措施，如磁盘阵列、双机备份等方式，以维护数据库系统的安全性、稳定性、可伸缩性和高性能。

证书发放申请的步骤参见下面介绍 Sun ONE CMS 的章节。

铁道部 CA 系统实施建议

我们推荐使用 Sun ONE Certificate Server 建立铁道部 CA 系统。在铁道部中可能遍布多个 CA 系统，可以部署 Sun ONE CMS 或其它供应商的 CMS，只要它们都发行 X509 证书。

CA 本身也需要一个证书来证明它自己的身份。给其它 CA 发放证书的 CA 称为根 CA。根 CA 可以从铁道部外的其它 CA 中获取证书，如安全部。根 CA 与其它 CA 发放证书的方式是相同的，如用 LDAP 为发布目录，使系统管理员以可以从目录中获取证书并安装到相应的 CA 上，参见下图。

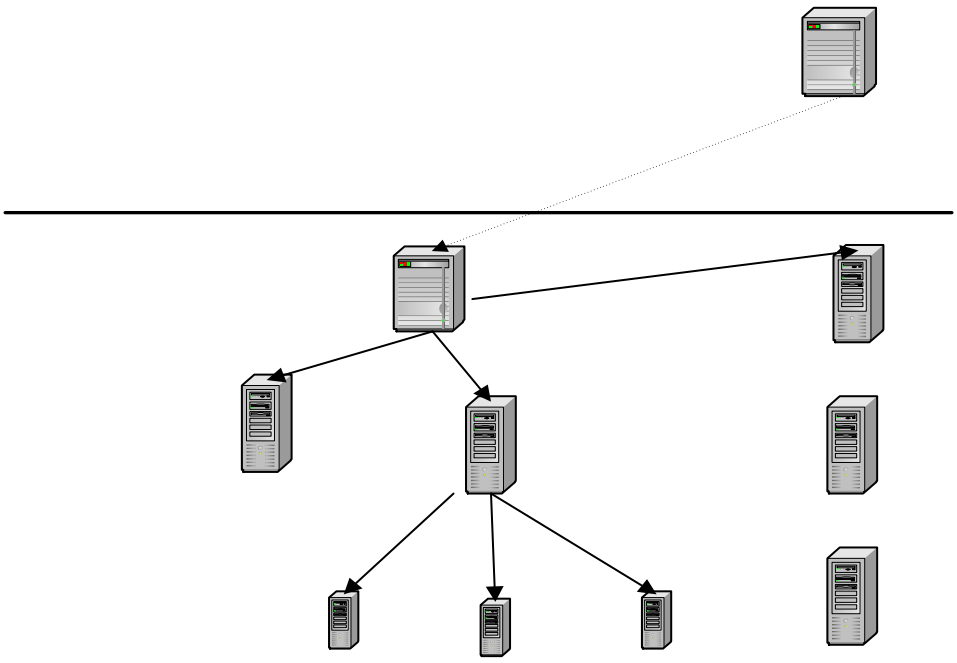


图 13、铁道部 CA 部署图

根 CA 负责铁道部中其它 CA 证书的发放，可能包括铁道部为电子商务应用程序发放证书的电子商务 CA 等。外部的 CA 验证根 CA 本身，其它 CA 信任根 CA，如可能为总部 CA 和分区域 CA。所有的 CA 都可以使用 Sun ONE CMS 或者其它供应商的产品。为管理方便，铁道部也可以只部署一个 CA。实际的部署情况将在 Sun 公司提供的专业服务中，与铁道部一起根据评估现存状况而确定。

4.2.6 铁道部门户系统

铁道部对应用系统的集成，实质上是为了在整合现有应用的基础上，为用户提供更多、更好、更安全的服务内容。近年来迅速发展的企业信息（服务）门户技术，其目的是为客户、合作伙伴和员工建立个性化的访问企业信息资源的入口，按不同用户组织专门的内容，通过及时向用户提供准确的信息来优化企业运作和提高生产力。即所谓，一个门户，针对不同客户提供多种服务。

Sun ONE Portal Server 帮助客户建立统一的信息门户，可以：

- 为合法用户访问企业内部资源提供一致的方式；
- 为用户提供个性化的信息；
- 员工通过门户的界面整合功能，提供统一的基于浏览器的应用访问界面；
- 支持单点登陆

构建铁道部门户系统需要进行的主要工作是：

- 统一的用户管理
- 用 Channel 实现应用系统内容的聚集和展现
- SSO

用户管理和 SSO 已经在前面的章节中予以了介绍。

如何通过 Channel 实现内容的集成

在系统开发中，可能需要开发多种后台应用程序的 Channel，应设立统一的开发原则，保证门户整体开发的一致性和扩展性。

我们认为开发原则是门户应主要关注构建显示窗口和基本内容的展现，主要的功能应放入后台应用程序，好处是松耦合，避免在 Channel 中过多实现后台应用操作性的功能，将来后台应用发生变化时，Channel 也要发生较大的调整。

参见下图，应再后台应用的表现层上做些配置，利于 Channel 的展现。

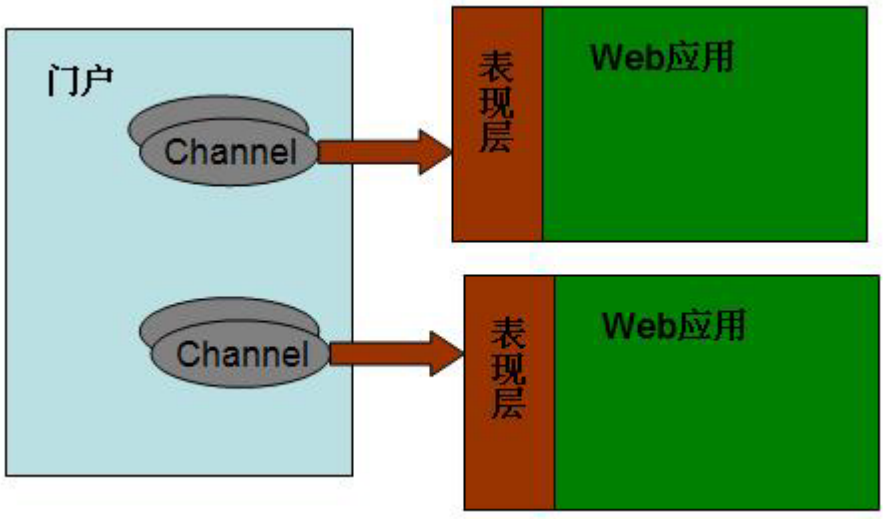


图 14、门户频道展现图

建议集中考虑用户内容集成的形式及频道展现的方式，应设计出 Channel 开发规范书。

1．Web 应用程序

当外部应用本身就是基于 Web 方式的应用时，Portal Server 通过 Http 或 Https 的方式与应用相连，获取相关内容后传输给浏览器即可。用户在该应用程序上的操作，Portal Server 可以获取其内容并转换为应用的 Http/Https 请求，由应用完成具体操作，最终由 Portal Server 将结果显示给用户。

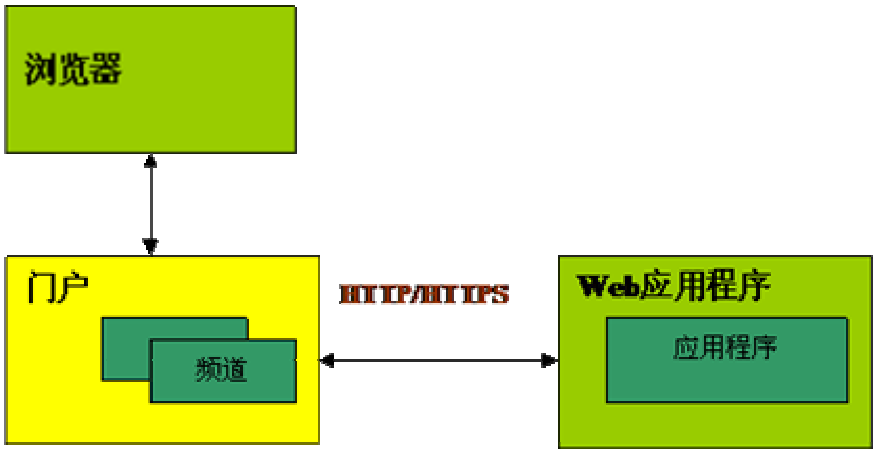


图 15、Web 应用程序的内容展现

2．提供远程 API 的应用

对于提供远程 API（如 JDBC/RPC）功能的应用，Portal Server 可直接调用 API 获取应用系统的内容及进行相关操作。浏览器将用户请求传递给 Portal，Portal 调用应用系统的 API，并将处理结果传回浏览器。这种方式增加 Portal 一端的开发工作量，造成 Channel 和后台应用都数据冗余，应尽量少采用，而应对外部应用程序做一些调整，参见上面所说的表现层集成方法。

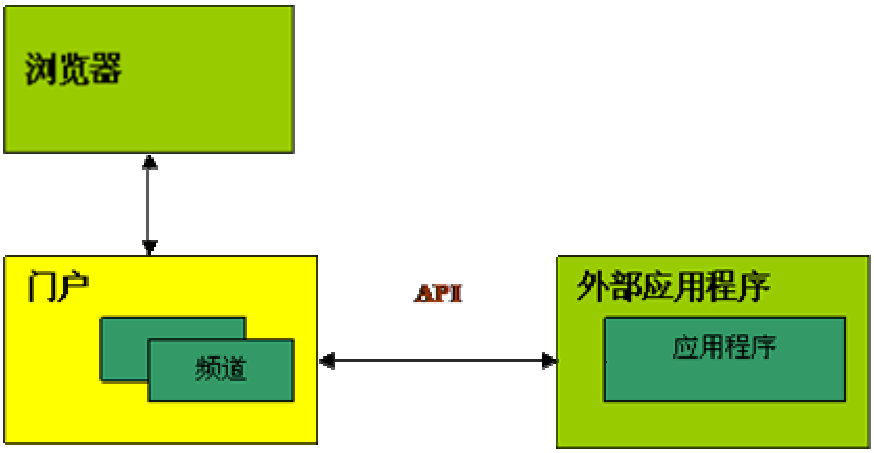


图 16、远程 API 应用的内容展现

3．其它应用系统

对于其它类型应用系统的内容连接主要通过应用服务器或集成服务器中间件的方式来实现。应用服务器或集成服务器对各类应用提供可相连的适配器 Adapter。Adapter 运用 JCA、SOAP、CORBA 及 SOCKET 等技术与外部应用相连。主要流程为浏览器将用户请求传递给 Portal，Portal 发送 HTTP/HTTPS 请求至应用服务器或集成服务器。应用服务器或集成服务器接收请求并调用 Adapter，由 Adapter 连接外部应用实现操作。最后 Portal 将其从应用服务器或集成服务器接收的结果传回用户界面。

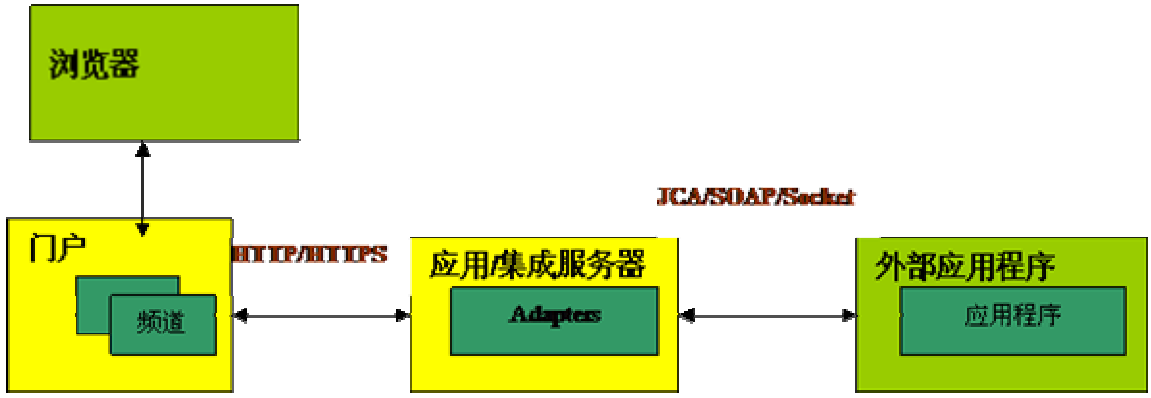


图 17、其它应用系统的内容展现

4.3 支持方案的产品描述

Sun ONE 已经提供了多种强有力的软件产品支持应用程序安全框架的方案，如 Identity Server、Directory Server、Portal Server、Certificate Server 等。本节介绍方案中采用的 Sun ONE 产品、NSS/JSS 工具包的原理和主要特性。

关于 Sun ONE 产品的详细介绍，请参见方案建议书附件中的 2.2 节。包括：

- Sun ONE 目录服务器 5.0
- Sun ONE Web 服务器企业版本
- SunTM ONE 门户服务器 6.0

- Sun™ ONE 认证管理系统（Certificate Management System）
- SunTM ONE 目录代理服务器 5.0（Directory Proxy Server 5.0）
- SunTM ONE Web 代理服务器（Web Proxy Server）
- SunTM ONE Web Identity Server

4.3.1 NSS/JSS 工具包

为在应用程序中支持 SSL、S/MIME 或其它 Internet 安全标准，可以使用 Network Security Services (NSS)实现铁道部的安全特性。**源代码开放的 NSS** 提供了对加密库的完整实现，Netscape、Sun 和其它公司在许多产品中使用了该库，包括：

- Netscape 6 浏览器
- AOL 战略业务方案产品包括 Netscape Certificate Management System、Netscape Enterprise Server、Netscape Directory Server 和 Netscape Messaging Server 等
- Sun ONE 产品包括 Directory Proxy Server、Certificate Server、Portal Server, Messaging Server 和 Application Server 等
- Netscape Personal Security Manager，它是一个客户端模块，代表其它应用程序进行加密操作。

NSS 提供：

- 验证过的架构 – Sun 在开发自己的产品时就使用了 NSS，这意味者自从 Internet 早期开始到现在，已经有数百万用户在使用 NSS。
- 协同性 – NSS 是一个对 SSL 2.0/3.0 安全标准的完全实现，与目前存在的大多数 Web 浏览器和 Web 服务器兼容。支持开放标准，如 SSL、X.509 v3 证书和 RSA 加密等，意味着 NSS 可以帮助你的客户端或者服务器应用程序与 Internet 上的其它部分实现安全连接。
- 灵活性 – 跨平台的 NSS 设计允许你的应用程序根据用户的需要而扩展或更改。可通过针对密码 Token 的 PKCS#11 标准结合使用硬件加速和智能卡。这种灵活性和对某种密码技术的独立性意味着可以根据需要定制我们的安全方案。

使用 NSS/ JSS 的主要好处在于铁道部拥有所有加密解密功能和 SSL 实现的源代码。铁道部可以进一步开发和评估这些代码，不仅确保安全性，而且可以使用它们作为产品商业化的基础。

4.3.2 Sun ONE Identity Server 工具包

我们建议铁道部安全框架的的核心部分基于 Sun ONE Identity Server。Sun ONE Identity Server 是一个全面的数字身份系统，提供策略服务，管理服务，安全服务和目录服务。它简化了身份的创建和管理，认证和访问策略的管理和执行。

Identity Server 的 Policy 模块包含了一些组件和服务。可以说，Identity Server 遵循着三层结构，Directory 为数据层，Policy Server 为中间层以及运行在 Web container 中的 Agents。

Identity Server 的功能架构图如下：

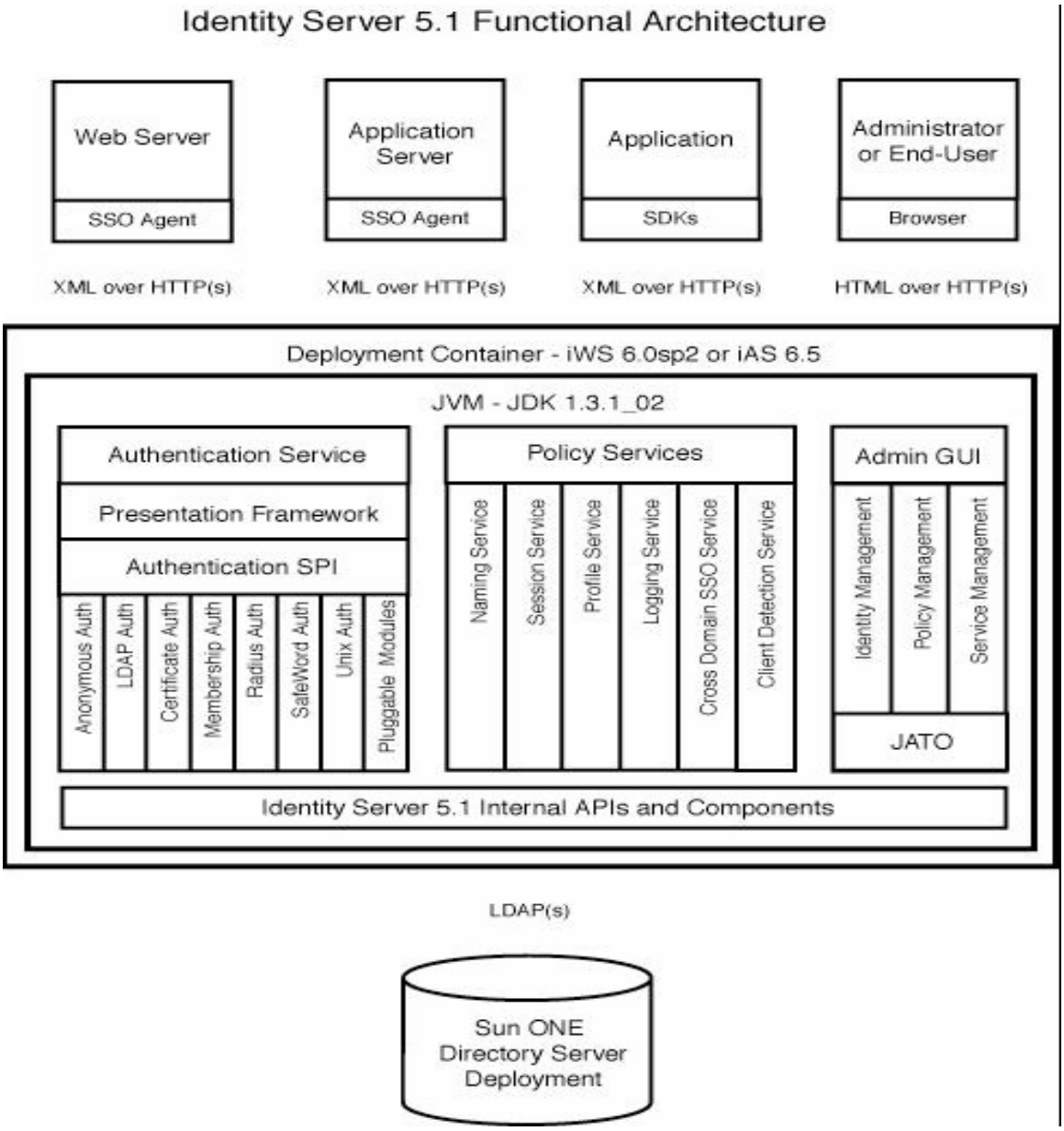


图 18、Identity Server 功能架构图

Directory Server: 作为一个给用户交付 Policy 的机制。这些 policies 中有允许、拒绝和 not-enforced URL 的列表。

Policy Services: 包含以下核心服务

- Naming 服务：给 Agents 提供 Identity Server 可用的服务、SSO tokens 的解密等。
- Logging 服务：提供集中式的 logging 机制。
- Authentication 服务：提供集中式的鉴权机制。
- Session 服务：创建和维护用户在 Identity Server 中的 SSO session。
- Profile 服务：提供关于用户的信息，比如用户的 Policy。

Agents: Identity Server 与 Agent Pack 一起提供 Agent，在 Web 服务器中执行 Policy。

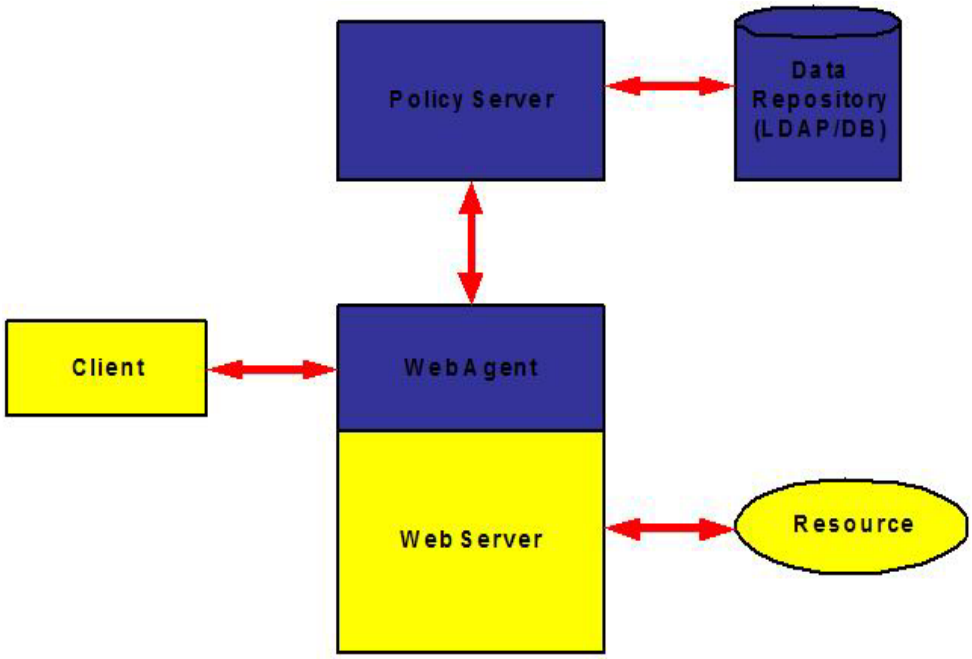


图 19、Agent 示意图

下表描述了 Sun ONE Identity Server 的主要组成

表 1：Sun ONE Identity Server 组成描述

组成	描述
认证	认证组件提供： • 认证框架 • 认证模块的插入式界面 • 认证用户和策略的 http/html 界面
SSO	提供 Web 应用程序的 SSO 方案。它为 Java 和非 Java 应用程序定义了 SSO API
服务管理	提供 Identity Server 的服务的管理框架。它定义了一个服务的 XML DTD，也提供服务管理的 Java API
身份管理	提供用户、角色、组、和组织管理，如创建、删除和修改等。该组件基于 Directory Server 5.1 的 CoS 特性。它也提供了 Java API
策略管理	提供了对资源策略的管理方案(定义、修改和清除)，以及确定用户对资源的权限
策略 Agents	为标准的服务器，如 Web 服务器和应用服务器提供 Agent 模块，例如 Web agent for Sun Web Server
管理服务	为身份和策略管理提供用户界面。它了定义不同类型的管理员，这些管理员在创建和管理用户、组、角色、组织、服务和策略上有不同的权限。
客户端确定	为了支持各种内容类型如 HTML 和 WML，提供一些 Java 类确定客户端类型。Identity Serve 内部的组件使用这些 Java 类决定产生何种内容。
工具	提供一些可以被各种类型的内部组件共用

	的 Java 类
日志	为 Identity Server 内部各种组件提供日志服务，提供 Java API 帮助记录事件，支持基于文件和基于 JDBC 的存储方式
安装程序	提供在 W2K 和 Solaris 上 Identity Server 的安装。W2K 上的安装程序基于 SetupSDK，而 Solaris 上的安装程序基于命令行
操作系统	支持 Solaris 和 Windows
Sun ONE Web Server (iWS)	iWS 包含在 Identity Server/iWS 版本中
Sun ONE Directory Server (iDS)	提供了 Identity Server 应用和服务的数据存储。它已经捆绑在 Identity Server 产品中
JSS/NSS	NSS/JSS 提供了对 NSS SSL 库的 Java 实现。Identity Server 用该类库实现 SSL 连接
JAXP	Java API for XML Processing 提供了 XML 解析和 XSLT 处理功能。该组件捆绑在 Identity Server 中
SetupSDK	Identity Server 的 W2K 安装程序基于 SetupSDK。该组件捆绑在 Identity Server 的 W2K 版本中
JDK	为 Identity Server 及其组件提供运行环境。捆绑 JDK 的主要原因在于 JATO 需要使用比 Application Server 新的 JDK 版本。
JATO	用作 Identity Server 管理控制台
SMPO	IDENTITY SERVER admin console uses it for its presentation.

下表描述了 Identity Server 的主要服务

Services	Description
认证服务(html/http(s))	为鉴别用户和发放 SSO Token 提供 Html/Http(s)界面。认证框架提供了一个可以插入式架构，允许客户开发自己的认证模块
策略服务 (xml/http(s))	为获得策略和用户信息提供了 XML/HTTP(s)界面。
管理图形用户界面 (html/http(s))	为 Web 浏览器提供了管理用户、策略和服务的 Html/Http(s) 界面。服务可以被所有的用户所使用。该服务用 Identity Server SDKs 如身份管理 SDK、服务管理 SDK 等完成表现层的功能
Java API	
认证 SDK	提供 Java API，使客户可以开发自己的认证模块，并插入到 Identity Server 认证模块中
SSO SDK	为验证 SSO Token 和维护用户的信任状提供 Java API
日志 SDK	提供日志 Java API，支持基于文件和 JDBC 两种方式
身份管理 SDK	提供创建和管理用户。角色、足、组织等功能的 Java API。使用 Directory Server 存储这些对象
策略管理 SDK	为策略结果的获取和设置提供 Java API
服务管理 SDK	提供注册和反注册服务的 Java API
CDM SDK	提供 Java 类确定客户端类型从而支持各种类型内容如 HTML 或 WML
工具 SDK	提供 Identity Server 内部组件共用的 Java 类

Web agents	提供基于 URL 的访问执行方式。它联系策略服务，获得用户和策略信息，也确认 SSO token。Web agents 可以安装在许多 Web 服务器上。
命令行界面	提供名为 *amadmin* 的命令行界面，做三种类型的操作：服务规划和元数据注册、身份管理和策略管理

4.3.3 Sun ONE CMS

Sun Certificate Management System 是一个基于证书的高扩展性安全方案，构建在 Sun Directory Server 的用户管理和访问控制基础之上。我们建议铁道部部署 PKI 做为完整用户认证方案的一个部分，使用证书管理系统的模块技术和管理架构，以及它的定制化和与非 PKI 认证系统的扩展能力。

下图展现了 Sun 证书管理系统的主要组件：

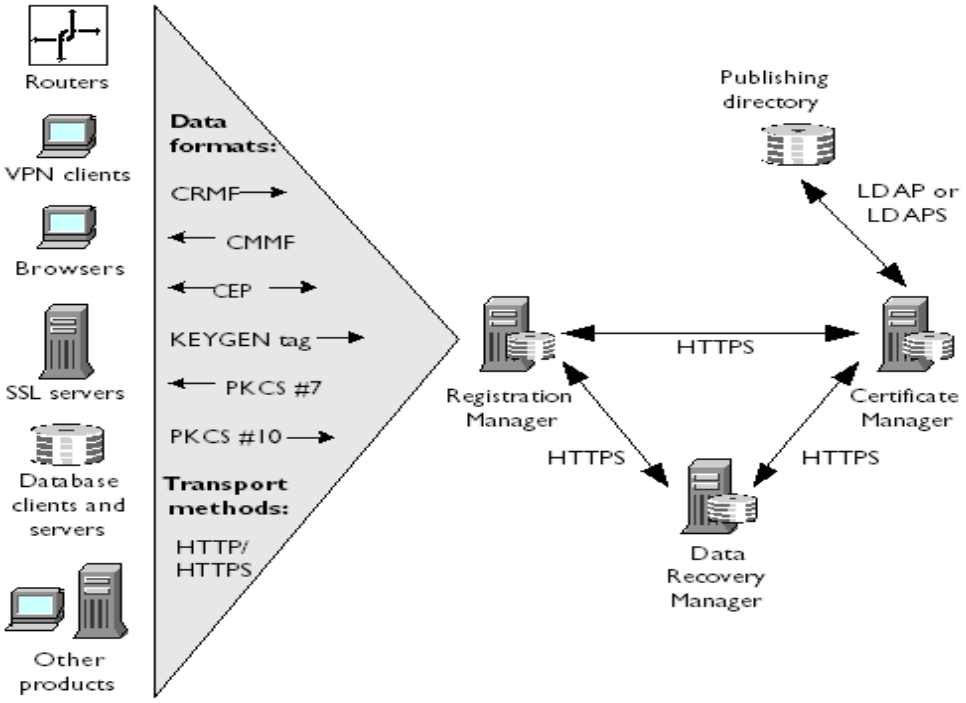


图 20、CMS 组件图

- 注册管理器(RA)提供认证、执行策略以及标明证书请求并发送到 CA
- 证书管理器签署和发放证书，也维护一个发放证书的数据库，以便追踪证书的恢复、过期和撤销。
- 数据恢复管理器是一个可选模块，可以用作归档密钥。通常当用户丢失了密钥或员工离职后公司需要恢复密钥时使用该模块。
- 支持注册和恢复协议的数据格式
  - CRS (证书请求语法/证书注册协议) 请求/响应格式，用于 VPN 客户端、路由器、硬件防火墙的联合
  - CRMF/CMMF – 一般用在双密钥对的请求
  - CRMF = 证书管理请求格式 = 从客户端到服务器的请求
  - CMMF = 证书管理消息格式 = 从服务器到客户端的响应

- KEYGEN tag – 浏览器用它放置证书请求
- PKCS #7 – 服务器端的证书回复
- PKCS #10 – 证书请求语法
- PKCS #11 – 硬件安全模块(HSMs)的标准，允许在硬件 Token 中存储签署的证书和 SSL 密钥
- OCSP – 在线证书状态协议 –向 CA 放置实时请求，确定是否某种证书在 a CRL – 过期或者撤销?
- FIPS 140-1 Level 3 – 政府标准，它规定一个硬件 Token 必须达到怎样的安全性，以及证书软件如何与硬件 Token 相交互。

图 14 是证书发放过程的简要示意图，针对铁道部的详细过程描述将作为 Sun 专业服务的一个组成部分。

1. 用户用注册管理器填写一个注册表格
2. 当用户填写完表格并提交，客户端产生一对密钥。
3. 注册管理器基于策略验证表格内的信息,向证书管理器提交一个签名证书的请求。
4. 证书管理器基于证书管理策略验证注册管理器
5. 如果证书管理器的策略允许立即签署该请求，请求提交到注册管理器而后，到用户(在同样的会话中)。注册管理器也可以选择发布证书到组织的目录中。
6. 如果证书管理器的策略需要其它信息，那么用户在以后需要返回去重获其证书。或者用户需要用证书请求号向注册管理器查询是否证书已经发放，或者配置注册管理器，使得证书获取就绪时，以电子邮件的方式通知。
7. 如果设置证书管理器去归档用户的私钥，运行在注册管理器上的一个 JavaScript 程序在客户端将产生两个密钥对并提取公钥。私钥将和数据恢复管理器的公钥进行包装，并提交到数据恢复管理器上。用户的公钥是证书收据的一个组成部分。数据恢复管理器检查私钥与公钥是否匹配，确保正确的密钥已归档，并将收据发送到注册管理器。
8. 只针对远程撤销,由数据恢复管理器发放的证书收据用作证书签署请求的一部分。

注册管理器向数据恢复管理器提交证书签署请求。

9. 依据策略，最终用户可以直接与数据恢复管理器的管理员联系来重获其密钥

以下是简化的证书发放流程示意图：

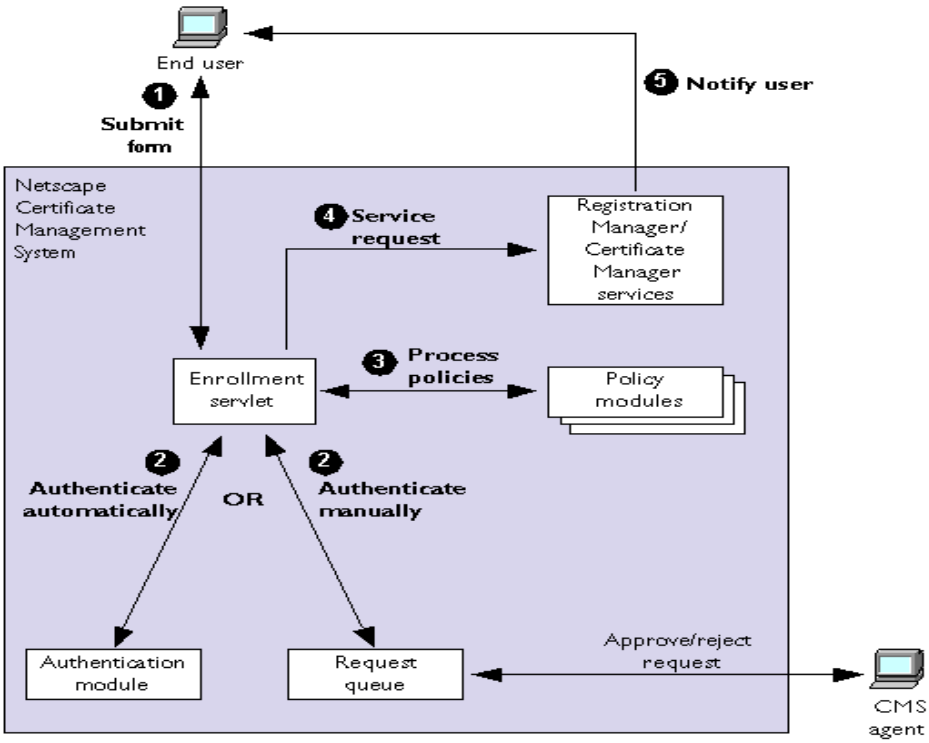


图 21、证书发布简要流程图

支持几种其它的证书发放方法，如面对面履行、通过电子邮件集中发放等。在同样的 PKI 域中可以按照安全和信任级别实现多种方法。服务器、应用程序和路由器也可以利用 PKI 基础架构，也存在自动化的证书请求、发放、撤销以及恢复的方法。对这些方法的详细阐述将在咨询服务中进行。

5 软硬件产品清单

5.1 Sun 硬件产品清单

5.1.1 试点工程阶段硬件设备清单

1.0	**内部网络A类访问控制系统平台：10套，每套含Sun Fire V880服务器两台，每台配置4颗900MHz CPU/8GB内存，6x73.4GB硬盘。**		
1.1	A30-WSF4-08GRF	Sun Fire V880服务器，配置 4 颗 900 MHz CPU, 8 GB内存, 6块73 GB, 1.0", 10,000 RPM, FC-AL 硬盘, DVD, 3 (N+1 redundant) 电源及冗余冷却风扇。	20
1.2	X1034A	四端口快速以太网卡（PCI接口）。Quad FastEthernet PCI Card (QFE) Quad FastEthernet is a high performance, high density network interface card. QFE provides immediate increase in bandwidth to the user in the PCI interface format.	20
1.3	X1141A	PCI千兆以太网卡，光纤接口。PCI Gigabit Ethernet Network Interface Card which provides Sun customers with the next generation Gigabit Ethernet product. The adapter has a single multimode fiber interface. It is a half size PCI form factor for 5 and 3.3 volt options.	20

1.4	X3768A	PGX64显卡，24位帧缓存，软件光盘，接口线缆，PCI接口。PGX64 24-bit Color Frame Buffer, Software on CD, Video adapter cable Solaris 2.5.1, 2.6, 7 & Solaris 8 (PCI systems only)	20
1.5	X386L	服务器主机电源线	30
1.6	X6758A	双端口Ultra 3 SCSI接口卡,PCI接口。PCI dual channel Ultra-3 differential SCSI host adapter	20
1.7	X9628A	Sun Fire V880服务器上架套件，用于将Sun Fire V880服务器安装到标准19"宽，39"高机架: Rackmount kit to mount system within a standard 19" wide, 39" deep rack. Requires 17 RU. Includes three (3) jumper/power extension cords, geography independent, part no. 530-3096-01.	20
1.8	SLS9S-120-W9YM	Solaris PC NetLink 1.2 捆绑软件，用于所有新服务器，无需使用许可，无限客户端访问。包括介质及HTML文档。Solaris PC NetLink 1.2 For all new Enterprise servers. no license required, Unlimited Client Access, Media Kit, Documentation in HTML. English and Localized Solaris 2.6, 7 and 8	20
1.9	SOLZS-08HB9AYD	Solaris 8 操作系统介质。Multilingual media (CD-ROM) with Simplified Install Documentation (latest release).	10
1.10	X3582A	USB键盘鼠标--International Type 6 Country Kits Chinese with USB interface	10
1.11	X7137A	18.1" TFT LCD液晶彩色显示器(相当于20" CRT), 1280x1024 @ 60/76Hz, 模拟RGB接口,数字DVI接口, DVI-D, 13W3,以及HD15视频线。	10

1.12	X386L	显示器电源线	10
2.0	**A类共享磁盘阵列，10套：Sun StorEdge D2盘阵，每两台服务器共享一套，每套配置8x36.4GB硬盘**		
2.1	SG-XARYDB196A-145G	145-GB (4 x 36.4-Gbyte 10K RPM硬盘) Sun StorEdge D2盘阵,机架型, 双总线, 每个总线有2个LVD Ultra 160 SCSI接口连接主机, 4个风扇, 2电源模块.--145-GB (4 x 36.4-Gbyte 10K RPM disks) Sun StorEdge D2, rackmount, dual bus, 2 LVD Ultra160 SCSI to host ports per bus, 2 fantrays (4 fans), 2 power supplies. Standard Configuration	10
2.2	X3830B	4米SCSI线（4-meter, Ultra VHDCI/VHDCI 68-pin cable）	20
2.3	X5250A	Ultra 3-SCSI内置硬盘，用于D2盘阵--Internal 36.4-Gbyte, 10Krpm Ultra 3 SCSI, LVD disk drive, 1" high, with barrier plate	40
3.0	**内部网络B类访问控制系统平台：1套，每套含Sun Fire V480服务器两台，每台配置4颗900MHz CPU/8GB内存，2x36.4GB硬盘。**		
3.1	A37-WSPF4-08GQB	Sun Fire V480服务器，配置4颗900MHz处理器，8GB内存,2块36GB硬盘(1.0", 10,000 RPM, FC-AL接口硬盘),DVD, 2电源模块.	2
3.2	X1034A	四端口快速以太网卡（PCI接口）。Quad FastEthernet PCI Card (QFE) Quad FastEthernet is a high performance, high density network interface card. QFE provides immediate increase in bandwidth to the user in the PCI interface format.	2

3.3	X1141A	PCI千兆以太网卡，光纤接口。PCI Gigabit Ethernet Network Interface Card which provides Sun customers with the next generation Gigabit Ethernet product. The adapter has a single multimode fiber interface. It is a half size PCI form factor for 5 and 3.3 volt options.	4
3.4	X3768A	PGX64显卡，24位帧缓存，软件光盘，接口线缆，PCI接口。PGX64 24-bit Color Frame Buffer, Software on CD, Video adapter cable Solaris 2.5.1, 2.6, 7 & Solaris 8 (PCI systems only)	2
3.5	X386L	服务器主机电源线	4
3.6	X6758A	双端口Ultra 3 SCSI接口卡,PCI接口。PCI dual channel Ultra-3 differential SCSI host adapter	2
3.7	SOLZS-08HB9AYD	Solaris 8 操作系统介质。Multilingual media (CD-ROM) with Simplified Install Documentation (latest release).	1
3.8	X3582A	USB键盘鼠标--International Type 6 Country Kits Chinese with USB interface	1
3.9	X7137A	18.1" TFT LCD液晶彩色显示器(相当于20" CRT)，1280x1024 @ 60/76Hz，模拟RGB接口,数字DVI接口, DVI-D, 13W3,以及HD15视频线。	1
3.10	X386L	显示器电源线	1
4.0	**B类共享磁盘阵列1套：Sun StorEdge D2盘阵，每两台服务器共享一套，每套配置8x36.4GB硬盘**		

4.1	SG-XARYDB196A-145G	145-GB (4 x 36.4-Gbyte 10K RPM硬盘) Sun StorEdge D2盘阵,机架型, 双总线, 每个总线有2个LVD Ultra 160 SCSI接口连接主机, 4个风扇, 2电源模块.--145-GB (4 x 36.4-Gbyte 10K RPM disks) Sun StorEdge D2, rackmount, dual bus, 2 LVD Ultra160 SCSI to host ports per bus, 2 fantrays (4 fans), 2 power supplies. Standard Configuration	1
4.2	X3830B	4米SCSI线（4-meter, Ultra VHDCI/VHDCI 68-pin cable）	2
4.3	X5250A	Ultra 3-SCSI内置硬盘，用于D2盘阵--Internal 36.4-Gbyte, 10Krpm Ultra 3 SCSI, LVD disk drive, 1" high, with barrier plate	4
5.0	**外网访问控制服务器：8套，每套含Sun Fire V480服务器两台，每台配置4颗900MHz CPU/8GB内存，2x36.4GB硬盘。**		
5.1	A37-WSPF4-08GQB	Sun Fire V480服务器，配置4颗900MHz处理器，8GB内存,2块36GB硬盘(1.0", 10,000 RPM, FC-AL接口硬盘),DVD, 2电源模块.	16
5.2	X1034A	四端口快速以太网卡（PCI接口）。Quad FastEthernet PCI Card (QFE) Quad FastEthernet is a high performance, high density network interface card. QFE provides immediate increase in bandwidth to the user in the PCI interface format.	16
5.3	X1141A	PCI千兆以太网卡,光纤接口。PCI Gigabit Ethernet Network Interface Card which provides Sun customers with the next generation Gigabit Ethernet product. The adapter has a single multimode fiber interface. It is a half size PCI form factor for 5 and 3.3 volt options.	32

5.4	X3768A	PGX64显卡，24位帧缓存，软件光盘，接口线缆，PCI接口。PGX64 24-bit Color Frame Buffer, Software on CD, Video adapter cable Solaris 2.5.1, 2.6, 7 & Solaris 8 (PCI systems only)	16
5.5	X386L	服务器主机电源线	32
5.6	X6758A	双端口Ultra 3 SCSI接口卡,PCI接口。PCI dual channel Ultra-3 differential SCSI host adapter	16
5.7	SOLZS-08HB9AYD	Solaris 8 操作系统介质。Multilingual media (CD-ROM) with Simplified Install Documentation (latest release).	8
5.8	X3582A	USB键盘鼠标--International Type 6 Country Kits Chinese with USB interface	8
5.9	X7137A	18.1" TFT LCD液晶彩色显示器(相当于20" CRT)，1280x1024 @ 60/76Hz, 模拟RGB接口,数字DVI接口, DVI-D, 13W3,以及HD15视频线。	8
5.10	X386L	显示器电源线	8
6.0	**Sun 72"标准大机柜，安装试点阶段设备，共21个大机柜**		
6.1	SG-XARY030A	72"标准机柜(72-inch StorEdge Expansion Rack w/ 2 power sequencers and cables The StorEdge Expansion Rack is intended for a variety of Products . The rack is 24" wide and 72" tall. This rack will include power sequencers and power cables.)	**21**
6.2	X9818A	72"机柜前门	**21**
6.3	X3859A	72"机柜电源线	**42**

5.1.2 工程推进阶段硬件设备清单

1.0	**内部网络A类访问控制系统平台：26套，每套含Sun Fire V880服务器两台，每台配置4颗900MHz CPU/8GB内存，6x73.4GB硬盘。**		
1.1	A30-WSF4-08GRF	Sun Fire V880服务器，配置 4 颗 900 MHz CPU, 8 GB内存, 6块73 GB, 1.0", 10,000 RPM, FC-AL硬盘, DVD, 3 (N+1 redundant) 电源及冗余冷却风扇。	52
1.2	X1034A	四端口快速以太网卡（PCI接口）。Quad FastEthernet PCI Card (QFE) Quad FastEthernet is a high performance, high density network interface card. QFE provides immediate increase in bandwidth to the user in the PCI interface format.	52
1.3	X1141A	PCI千兆以太网卡，光纤接口。PCI Gigabit Ethernet Network Interface Card which provides Sun customers with the next generation Gigabit Ethernet product. The adapter has a single multimode fiber interface. It is a half size PCI form factor for 5 and 3.3 volt options.	52
1.4	X3768A	PGX64显卡，24位帧缓存，软件光盘，接口线缆，PCI接口。PGX64 24-bit Color Frame Buffer, Software on CD, Video adapter cable Solaris 2.5.1, 2.6, 7 & Solaris 8 (PCI systems only)	52
1.5	X386L	服务器主机电源线	156
1.6	X6758A	双端口Ultra 3 SCSI接口卡，PCI接口。PCI dual channel Ultra-3 differential SCSI host adapter	52

1.7	X9628A	Sun Fire V880服务器上架套件，用于将Sun Fire V880服务器安装到标准19"宽，39"高机架：Rackmount kit to mount system within a standard 19" wide, 39" deep rack. Requires 17 RU. Includes three (3) jumper/power extension cords, geography independent, part no. 530-3096-01.	52
1.8	SLS9S-120-W9YM	Solaris PC NetLink 1.2 捆绑软件，用于所有新服务器，无需使用许可，无限客户端访问。包括介质及HTML文档。Solaris PC NetLink 1.2 For all new Enterprise servers. no license required, Unlimited Client Access, Media Kit, Documentation in HTML. English and Localized Solaris 2.6, 7 and 8	52
1.9	SOLZS-08HB9AYD	Solaris 8 操作系统介质。Multilingual media (CD-ROM) with Simplified Install Documentation (latest release).	26
1.10	X3582A	USB键盘鼠标--International Type 6 Country Kits Chinese with USB interface	26
1.11	X7137A	18.1" TFT LCD液晶彩色显示器(相当于20" CRT)，1280x1024 @ 60/76Hz, 模拟RGB接口,数字DVI接口, DVI-D, 13W3,以及HD15视频线。	26
1.12	X386L	显示器电源线	26
2.0	A类共享磁盘阵列，26套：Sun StorEdge D2盘阵，每两台服务器共享一套，每套配置8x36.4GB硬盘		

2.1	SG-XARYDB196A-145G	145-GB (4 x 36.4-Gbyte 10K RPM硬盘) Sun StorEdge D2盘阵,机架型, 双总线, 每个总线有2个LVD Ultra 160 SCSI接口连接主机, 4个风扇, 2电源模块.--145-GB (4 x 36.4-Gbyte 10K RPM disks) Sun StorEdge D2, rackmount, dual bus, 2 LVD Ultra160 SCSI to host ports per bus, 2 fantrays (4 fans), 2 power supplies. Standard Configuration	26
2.2	X3830B	4米SCSI线（4-meter, Ultra VHDCI/VHDCI 68-pin cable）	52
2.3	X5250A	Ultra 3-SCSI内置硬盘，用于D2盘阵--Internal 36.4-Gbyte, 10Krpm Ultra 3 SCSI, LVD disk drive, 1" high, with barrier plate	104
3.0	**内部网络B类访问控制系统平台：28套，每套含Sun Fire V480服务器两台，每台配置4颗900MHz CPU/8GB内存，2x36.4GB硬盘。**		
3.1	A37-WSPF4-08GQB	Sun Fire V480服务器，配置4颗900MHz处理器，8GB内存,2块36GB硬盘(1.0", 10,000 RPM, FC-AL接口硬盘),DVD, 2电源模块.	56
3.2	X1034A	四端口快速以太网卡（PCI接口）。Quad FastEthernet PCI Card (QFE) Quad FastEthernet is a high performance, high density network interface card. QFE provides immediate increase in bandwidth to the user in the PCI interface format.	56
3.3	X1141A	PCI千兆以太网卡,光纤接口。PCI Gigabit Ethernet Network Interface Card which provides Sun customers with the next generation Gigabit Ethernet product. The adapter has a single multimode fiber interface. It is a half size PCI form factor for 5 and 3.3 volt options.	112

3.4	X3768A	PGX64显卡，24位帧缓存，软件光盘，接口线缆，PCI接口。PGX64 24-bit Color Frame Buffer, Software on CD, Video adapter cable Solaris 2.5.1, 2.6, 7 & Solaris 8 (PCI systems only)	56
3.5	X386L	服务器主机电源线	112
3.6	X6758A	双端口Ultra 3 SCSI接口卡,PCI接口。PCI dual channel Ultra-3 differential SCSI host adapter	56
3.7	SOLZS-08HB9AYD	Solaris 8 操作系统介质。Multilingual media (CD-ROM) with Simplified Install Documentation (latest release).	28
3.8	X3582A	USB键盘鼠标--International Type 6 Country Kits Chinese with USB interface	28
3.9	X7137A	18.1" TFT LCD液晶彩色显示器(相当于20" CRT), 1280x1024 @ 60/76Hz, 模拟RGB接口,数字DVI接口, DVI-D, 13W3,以及HD15视频线。	28
3.10	X386L	显示器电源线	28
4.0	**B类共享磁盘阵列28套：Sun StorEdge D2盘阵，每两台服务器共享一套，每套配置8x36.4GB硬盘**		
4.1	SG-XARYDB196A-145G	145-GB (4 x 36.4-Gbyte 10K RPM硬盘) Sun StorEdge D2盘阵,机架型, 双总线, 每个总线有2个LVD Ultra 160 SCSI接口连接主机, 4个风扇, 2电源模块.--145-GB (4 x 36.4-Gbyte 10K RPM disks) Sun StorEdge D2, rackmount, dual bus, 2 LVD Ultra160 SCSI to host ports per bus, 2 fantrays (4 fans), 2 power supplies. Standard Configuration	28
4.2	X3830B	4米SCSI线（4-meter, Ultra VHDCI/VHDCI 68-pin cable）	56

4.3	X5250A	Ultra 3-SCSI内置硬盘，用于D2盘阵--Internal 36.4-Gbyte, 10Krpm Ultra 3 SCSI, LVD disk drive, 1" high, with barrier plate	112
5.0	**外网访问控制服务器：26套，每套含Sun Fire V480服务器两台，每台配置4颗900MHz CPU/8GB内存，2x36.4GB硬盘。**		
5.1	A37-WSPF4-08GQB	Sun Fire V480服务器，配置4颗900MHz处理器，8GB内存,2块36GB硬盘(1.0", 10,000 RPM, FC-AL接口硬盘),DVD, 2电源模块.	52
5.2	X1034A	四端口快速以太网卡（PCI接口）。Quad FastEthernet PCI Card (QFE) Quad FastEthernet is a high performance, high density network interface card. QFE provides immediate increase in bandwidth to the user in the PCI interface format.	52
5.3	X1141A	PCI千兆以太网卡,光纤接口。PCI Gigabit Ethernet Network Interface Card which provides Sun customers with the next generation Gigabit Ethernet product. The adapter has a single multimode fiber interface. It is a half size PCI form factor for 5 and 3.3 volt options.	104
5.4	X3768A	PGX64显卡，24位帧缓存，软件光盘，接口线缆，PCI接口。PGX64 24-bit Color Frame Buffer, Software on CD, Video adapter cable Solaris 2.5.1, 2.6, 7 & Solaris 8 (PCI systems only)	52
5.5	X386L	服务器主机电源线	104
5.6	X6758A	双端口Ultra 3 SCSI接口卡,PCI接口。PCI dual channel Ultra-3 differential SCSI host adapter	52

5.7	SOLZS-08HB9AYD	Solaris 8 操作系统介质。Multilingual media (CD-ROM) with Simplified Install Documentation (latest release).	26
5.8	X3582A	USB键盘鼠标--International Type 6 Country Kits Chinese with USB interface	26
5.9	X7137A	18.1" TFT LCD液晶彩色显示器(相当于20" CRT), 1280x1024 @ 60/76Hz, 模拟RGB接口,数字DVI接口, DVI-D, 13W3,以及HD15视频线。	26
5.10	X386L	显示器电源线	26
6.0	**Sun 72"标准大机柜，安装试点阶段设备，共21个大机柜**		
6.1	SG-XARY030A	72"标准机柜(72-inch StorEdge Expansion Rack w/ 2 power sequencers and cables The StorEdge Expansion Rack is intended for a variety of Products . The rack is 24" wide and 72" tall. This rack will include power sequencers and power cables.)	80
6.2	X9818A	72"机柜前门	80
6.3	X3859A	72"机柜电源线	160

5.2 Sun ONE 软件产品清单

Sun ONE Portal Server	PSED9-LCO-JA99	Sun ONE Portal Server, License Only, pricing is per CPU, no CPU minimum required
Sun ONE Portal Server: Secure Remote Access Pack	PSRD9-LCO-JA02	Sun ONE Portal Server: Secure Remote Access Pack, License Only, 5,000-9,999 users
Sun ONE Directory Server	DIRD9-LCO-JA01	Sun ONE Directory Server, License Only, pricing per entry, 1 - 199,999 entries
Sun ONE Web Proxy Server	PRXD9-LCO-JA99	Sun ONE Web Proxy Server, License Only, pricing per CPU
Sun ONE Identity Server	SISD9-LCO-JA01	Sun ONE Identity Server, License Only, pricing per entry, 1 - 49,999 entries
Sun ONE Certificate Server	CMSD9-LCO-JA01	Sun ONE Certificate Server, License Only, pricing per entry, 1 - 49,999 entries
Sun ONE Application Server, Standard Edition	SASDM-LCO-JA99	Sun ONE Application Server Standard Edition, Development and Deployment License, License Only, pricing per CPU

5.3 第三方产品

为了实现铁道部系统的安全，需要下列第三方产品：

1. 防火墙产品
2. 安全产品

   防病毒产品

   入侵检测

   日志分析软件
3. 物理隔离产品

6 Sun 提供的咨询服务内容描述

本章描述的是 Sun 提供的专业咨询服务的具体内容。

在方案建议书的前四章中阐述的是铁道部的安全技术方案，其中有一些内容是从中长期规划的角度建议的方案，例如，内容过滤，完整性保证等，将不会包含在这一章。另外，前四章中阐述的某些内容是第三方厂商或代理商提供的工作，因此，也不包括在这一章中。

6.1 项目管理咨询服务内容描述

Sun 将提供项目管理的咨询服务，与铁道部项目经理一起来管理整个项目，包括第三方硬软件厂商和代理商，以及铁道部的相关人员。SUN 将委任一位资深的项目经理参与项目的管理。他将代表 Sun，与铁道部项目经理和项目组一起对项目的进展和运作进行协商和决策，SUN 项目经理是 Sun 和铁道部、第三方厂商和代理商之间的主要联络人。

6.1.1 工作描述

项目管理咨询服务的工作内容如下：

1. 项目计划

- 和铁道部一起检查项目工作说明书内的工作及双方的合同责任；
- 制定项目计划；
- 根据项目计划，向 SUN 项目组成员分派任务及确定职责；
- 根据项目计划，通过铁道部项目经理向铁道部项目组分派任务；

- 确立项目文档和实施过程标准；

2. 项目跟踪与监控

- 通过铁道部项目经理与铁道部保持项目沟通；
- 根据项目计划，度量和评估项目进展情况；
- 如果出现与项目计划不同的变更，根据变更控制程序，和铁道部项目经理一起解决；
- 和铁道部项目经理一起核查和管理项目变更控制程序；
- 定期向铁道部项目经理提交状态报告；
- 协调和管理项目组人员的项目实施工作；

3. 项目检查会议

- 在项目组内部，定期按计划举行项目状态会议；
- 定期向项目协调领导委员会报告项目的进展情况。

6.1.2 工作交付文件

1. 项目计划

在项目实施的各个阶段(现状评估阶段、设计阶段、应用改造和部署阶段、测试阶段等)，将会制订更详尽的计划。

2. 项目状况报告

6.1.3 所需咨询顾问及其工作内容

对第一个点的试验项目，Sun 项目经理会全程参与，进行项目的管理和协调工作。

顾问	*数量(人)*	*人天*	*工作内容*	*备注*

Sun 资深项目经理	1	50	项目管理和协调工作	第一个点

对随后的推广项目，Sun 项目经理的参与时间会相应的递减。

6.2 应用集成咨询服务内容描述

6.2.1 用户管理和目录结构设计咨询服务

用户管理和目录结构设计咨询服务的目的是为了帮助铁道部客户建立一个目录系统，保存和管理包括公开密钥在内的用户身份认证信息。Sun 的资深专家将协助铁道部客户做下列工作：

- 目录服务的架构设计，并撰写相关文档
- 安装和部署目录服务系统，并撰写相关手册
- 目录服务的管理，并撰写相关文档

目录服务技术的咨询服务，总共需要 35 人天的工作量。

6.2.1.1 目录服务架构设计

Sun 公司专家帮助铁道部定义业务和技术需求，并基于需求设计目录服务架构和实施规划。主要工作内容包括：

- 目录信息评估
- 对支持目录服务的基础架构的评估
- 目录服务架构设计文档，包括：
  - 方案概述
  - 目录信息树高设计

- 安全和访问控制策略
- 目录复制、负载均衡和高可用性的策略
- 目录迁移、同步和共存策略

- 阶段性实现和部署规划
- 对建议架构的知识传授

工作量： 15 人天（1 人×15 天）

6.2.1.2 安装和部署目录服务软件

Sun 公司帮助铁道部在一个点上安装、配置和测试 Sun ONE Directory Server。主要工作内容包括：

- 对 Directory Server 部署的系统、网络和安全环境进行评估
- 安装和配置 Directory Server 的一个实例
- 系统功能的验证测试
- 建立 POC 原型
- 知识传授

对于组织机构而言，目录系统是每日运营的基础服务，如何有效地对其进行管理是重要的。Sun 公司地专家将帮助铁道部制定目录管理地策略和规程，包括：

- 目录服务的基本过程
- 目录服务的监控
- 目录系统的数据备份
- 目录系统的数据恢复
- 目录系统的日志管理

工作量： 15 人天（1 人×20 天）

用户管理和目录架构设计服务，所需咨询顾问及工作量：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
目录服务设计师（Directory services Architect）	1	15	DIT/Schema 设计，provisioning	第一个点
目录 IT 基础设施架构设计师（Directory IT Architect）	1	20	目录拓扑结构的设计，安装，配置，HA 设计等，目录管理的策略制定	
总共		35		

对随后的推广项目，咨询顾问参与的时间会相应的递减。

6.2.2 认证管理系统（CMS）咨询服务

铁道部已经购买和部署了 Sun CMS 作为其 CA 系统。依据铁道部的需求，Sun 公司提供 CMS 咨询服务使现有的 CMS 系统升级到最新版本，并建立适当的 PKI 管理流程和体系架构。主要工作内容包括：

- 建立证书发放的流程，并参照业界的最佳实践而实现
- 建立用户注册授权规范以及 CMS 的体系架构
- 与目录服务器的集成

所需咨询顾问及工作量：

顾问	*数量（人）*	*人天*	*工作内容*	*备注*
CMS 顾问	1	20	认证管理系统（CMS）咨询服务	第一个点

第一个点，共需要 20 人天（1 人×20 天）的工作量。

对随后的推广项目，咨询顾问参与的时间会相应的递减。

6.2.3 应用改造的咨询服务

应用改造咨询服务的目的是基于通用 PKI 的使用，帮助铁道部建立集中式的应用授权系统并实现 SSO 功能。应用改造的咨询服务，总共需要 90 人天的工作量。包括：

6.2.3.1SSO 的设计和 Web Agent 的开发

SSO 方案设计及 C/S 应用程序上 SSO Web agent 的开发。

需要 2 人，共 25 人天的工作量。

6.2.3.2 NSS/JSS 编程指导

C/S 应用程序上客户端应用改造的步骤，NSS/JSS 编程和编码规范的指导。

需要 1 人，35 人天的工作量。

6.2.3.3 服务器端应用程序改造指导

C/S 应用程序上服务器端应用改造的步骤和编码规范的指导。

需要 1 人，15 人天的工作量

6.2.3.4 Identity Server 的安装和部署指导

Sun 公司帮助铁道部在一个点上安装、配置和测试 Sun ONE Identity Server。

主要工作内容包括：

- 对 Identity Server 部署的系统、网络和安全环境进行评估

- 安装和配置 Identity Server 的一个实例
- 系统功能的验证测试
- 建立 POC 原型
- 知识传授

需要 1 人，15 人天的工作量。

应用改造的咨询服务，所需咨询顾问及工作量总结：

顾问	*数量（人）*	*人天*	*工作内容*	*备注*
应用设计师	2	25	SSO 设计和 web Agent 服务的设计	第一个点
应用设计师	1	35	NSS/JSS 编程指导	
应用设计师	1	15	服务器端的应用程序改造指导	
Identity Server 顾问	1	15	对 Identity Server 的安装和配置进行指导	
总共		90		

对随后的推广项目，咨询顾问参与的时间会相应的递减。

6.2.4 门户技术咨询服务

门户技术为 Web 和某类 TCP/IP 应用程序提供内容集成方式。在这些内容之间，门户也提供单点登录（SSO）功能。门户技术顾问协助铁道部客户将各种应用程序集成到统一的门户框架中。门户技术的咨询服务包括以下工作：

- 门户系统的架构设计，并撰写相关文档
- 安装和部署门户系统，并撰写相关手册

门户技术的咨询服务，总共需要 30 人天的工作量。

6.2.4.1 门户系统的架构设计

Sun 公司专家将收集、分析并确定用户对门户技术的具体需求，如个性化、成员管理、内容聚合、授权与认证等。基于这些信息，制定门户架构设计方案和实施计划。主要工作内容包括：

- 评估门户部署的现存的基础架构
- 门户系统的需求分析
- 门户架构文档的制定，包括：
  - 扩展性和可用性评估
  - 门户设计评估
  - 门户服务器的配置和容量规划
  - 对需要集成进门户系统的应用程序的技术评估
  - 根据需要集成的应用程序要求，设计单点登陆的架构方案(SSO)
  - 门户频道的实施策略
- 阶段性实施和部署计划
- 对建议架构的知识传授

需要 2 人，共 20 人天（2 人×10 天）的工作量。

6.2.4.2 门户系统的安装和部署指导

主要工作内容包括：

- 安装、配置和演示 Sun ONE Portal Server 的一个实例
- 设立门户系统的 POC 示例，包括

– 门户系统 UI 的配置

– 门户系统频道的开发，采用 URLScraper 和 JSPProvider 方式

- 相关知识的传授

需要 1 人，10 人天的工作量。

门户技术咨询服务，所需咨询顾问及工作量：

顾问	*数量（人）*	*人天*	*工作内容*	*备注*
门户技术顾问	2	20	门户系统的架构设计	第一个点
门户技术顾问	1	10	门户系统的安装和部署指导	
	总共	30		

对随后的推广项目，咨询顾问参与的时间会相应的递减。

6.3 网络安全咨询服务内容描述

针对铁道部网络安全的需求，Sun 推荐下列网络安全咨询服务：

13. 防火墙
14. 物理隔离系统
15. 入侵检测
16. 病毒防范
17. 关键服务器系统的安全
18. 紧急响应体系
19. 日志系统与审计
20. 安全策略

21. 安全流程

6.3.1 防火墙

6.3.1.1内容提纲

正如前面章节所述，防火墙的作用在于阻止对网络未经授权的访问。当允许对 Internet 完全、透明的访问时，防火墙起到保护铁道部内部资源的作用。防火墙也用于阻止未经授权的用户访问敏感信息或连接。

防火墙的基本原理对大多数专业人士和黑客来说比较容易理解。它的状态表追踪 TCP 会话，允许防火墙内的人员访问外部的 Internet，客户或合作伙伴访问公司信息，阻止黑客访问内部资源。

铁道部为了保持与外部的联系，必须开放一些端口和信息入口。例如，为了客户可以访问铁道部的 Web 服务器，必须开放端口 80 或 HTTP。

在 Internet 上，有许多工具可以帮助黑客利用这些条件。建议使用一个端口扫描程序 NMAP，可以扫描防火墙并发现进出网络的所有客利用端口。

6.3.1.2工具

在铁道部网络系统上，部署三类防火墙。分别是外部防火墙、内部防火墙和核心服务防火墙。我们建议每种防火墙都安装在业界最稳定的操作系统 Solaris 上。

Sun 公司建议采用第三方产品，并按照不同的部署需要选择不同产品，以满足国家相关法律法规对铁道部网络安全的要求：

- 外部防火墙 – 国内公司生产的防火墙产品
- 内部防火墙 – 国内或国外公司的防火墙产品
- 核心服务防火墙 –国内或国外公司的防火墙产品

6.3.1.3咨询流程

防火墙的咨询服务包括以下工作：

1．检查防火墙部署体系结构设计，包括防火墙在网络中的位置，可用性和可扩展性；

2．检查防火墙设置规则；

6.3.1.3.1防火墙部署体系结构检查

检查防火墙部署的位置，DMZ 体系结构，检查防火墙高可用性和负载平衡方案，检查防火墙的管理规定，如防火墙日志管理，防火墙安装区域，规则更动流程等。检查信任网络分段。

6.3.1.3.2 检查防火墙规则

根据铁道部网络安全策略和防火墙规则的业界最佳实践，检查防火墙规则。业界最佳实践的示例如下：

- 所有没有明确允许的都应该禁止
- 在规则集的顶端设置最通用的访问规则，明确规则应用的次序
- 尽量详细精确的定义防火墙规则
- 在同一个防火墙规则中避免使用相同的源和目的
- 最小化防火墙的规则数目，确认所有可以合并的规则均已合并
- 安装规则到特定的防火墙而不是安装到网关上
- 明确适当的定义缺省规则、标准规则
- 确保所有的出厂默认特性已经被关闭

所需咨询顾问及其人天估计：

顾问	*数量（人）*	*人天*	*工作内容*	*备注*
安全顾问	1	8	检查防火墙部署体系结构设计，包括防火墙在网络中的位置，可用性和可扩展性； 检查防火墙设置规则	第一个点
安全顾问	1	1		推广工程中的一个点

6.3.2 物理隔离系统

6.3.2.1内容提纲

物理隔离系统必须要考虑国家政策的符合性，以及系统的可信度。

物理隔离系统的目标是确保在不可信的外部网和内部网络之间没有物理或电子通路。

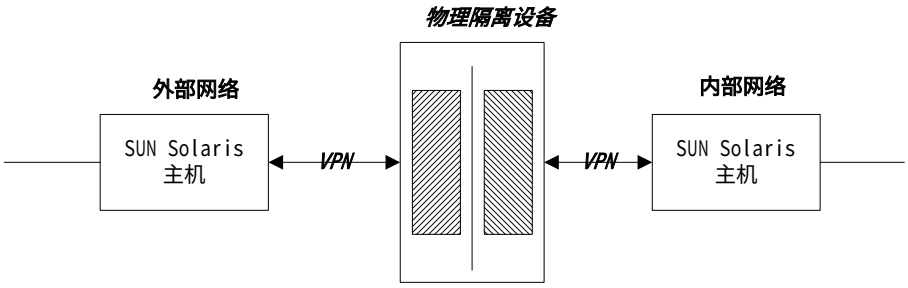
物理隔离系统通常包含电源供应、存储库和在一段时间内只可以一个端口的高速交换机。当外部服务器在硬件设备上装载应用程序级信息后，物理隔离系统中的交换机与外部系统切断连接，而连接到内部系服务器。

为保证物理隔离系统两方的服务器都宕机情况下系统仍然可以工作，在物理隔离系统和服务器之间需要使用 VPN。

6.3.2.2工具

Sun 公司建议物理隔离系统采用国内公司的第三方产品。

6.3.2.3咨询流程



基于图示意的物理隔离设备网络连接方式，Sun 提供的物理隔离系统的咨询服务包括以下工作：

1．检查网络结构设计，包括物理隔离设备在网络中的位置

2．部署并进行与物理隔离系统相连接的 Sun 系统的 VPN 的基本测试

所需咨询顾问及人天估计：

顾问	*数量（人）*	*人天*	*工作内容*	*备注*
技术顾问	1	15	检查网络结构设计，包括物理隔离设备在网络中的位置 部署并进行与物理隔离系统相连接的 Sun 系统的 VPN 的基本测试	第一个点
技术顾问	1	1		推广工程中的一个点

6.3.3 入侵检测（IDS）

6.3.3.1内容提纲

使用入侵检测软件通过自动检测网络数据流中潜在入侵，攻击和滥用方式。同时深入

了解系统整体安全性以及遵守的策略以及网络内部的运行情况。

Sun 建议采用第三方产品进行入侵检测，由第三方厂商或代理商安装、配置并测试入侵检测软件，并编制相应的文档。Sun 提供咨询服务，建立入侵检测策略，并审查入侵检测的有效性。

6.3.3.2工具

使用铁道部已有的入侵检测软件系统。

6.3.3.3咨询流程

入侵检测系统的咨询服务包括以下工作：

1. 制定入侵检测策略，管理流程；一些入侵检测基本策略和管理规程提纲如下：

   - 入侵检测应该实时连续进行，并建立全面的攻击方式库；
   - 字匹配扫描：定义表明可能会违反策略的字方式。这种方式可以防止了未经授权就通过 e-mail 或 Web 发送敏感数据等情况的发生；
   - 网络使用日志：网络管理员跟踪最终用户、应用程序等的网络使用情况。它有助于改进网络策略规划；
   - 远程管理：远程用户可以通过 TCP/IP 或调制解调器连接访问运行入侵检测软件的工作站，按照入侵检测软件管理员定义的许可内容，查看和监视入侵检测数据、修改规则和生成报告；
   - 入侵日志及分析：应指定日志归档地点，在档案中记录会话的规则。然后通过浏览器过滤、排序和查看归档信息，并创建详细的报告。

所需咨询顾问及人天估计：

顾问	*数量（人）*	*人天*	*工作内容*	*备注*
技术顾问	1	5	制定入侵检测策略，管理流程；	第 一 个

				点
技术顾问	1	1		推广工程中的一个点

6.3.4 病毒防范

6.3.4.1内容提纲

病毒检测服务器能扫描电子邮件消息(SMTP)、网页内容(HTTP)和文件内容(FTP)，检测和清除其所携带的病毒。

6.3.4.2工具

Sun 推荐第三方产品方案，所选择的软件应具有全面的病毒查杀功能，包括可执行文件、压缩文件、电子邮件、Office 文档、HTML 文档等多种文件类型内部的病毒。工具可以集检测、清除、治愈为一体，形成全面的反病毒机制。

6.3.4.3咨询流程

病毒扫描产品的咨询服务包括以下工作：

建立病毒防范规程和处理流程。下面是一个基本内容的示例提纲：

- 使用全公司统一的，可以获得技术支持的防病毒软件；
- 对可疑的不明来源的邮件的附件或宏文件的处理规程；
- 下载文件的规定；
- 直接的磁盘读/写共享的规定；
- 使用软盘的规程；

- 关键的数据和系统配置的备份和存储规定；
- 特定的运行状态和防病毒软件冲突的处理方式；
- 定期进行防病毒的检查。

所需咨询顾问及人天估计：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
安全顾问	1	3	建立病毒防范规程和处理流程。	第一个点
		0		推广工程中的一个点

6.3.5 关键服务器系统的安全咨询

6.3.5.1内容提纲

为了增强铁道部关键业务服务器的安全，Sun 建议在 Web 服务器、DNS 服务器、代理服务器、目录服务器上提供下列客户化的咨询服务：

1. 简化操作环境；
2. 确定操作系统补丁并及时更新
3. 追踪、侦测上述铁道部关键业务服务器的安全漏洞
4. Solaris 操作系统安全性固化

Sun 将审查和分析业务、技术和应用需求以建立配置规范，并遵循 Sun 的最佳实践实施这个配置。在 Solaris 操作系统安全性固化实施中培训铁道部的员工相关知识和技能。

6.3.5.2工具

推荐使用 Sun 专业的 Solaris 安全性工具包 JASS（JumpStart[tm] Architecture and Security Scripts）。JASS 提供灵活的可扩展的机制最小化、固化和保护 Solaris 操作环境，使 Solaris 系统的安全防护自动化处理。Sun 公司推荐定期追踪系统的安全漏洞。

JASS 以尽可能小的对主机系统的更动获得最大的作用，不依赖于主机使用的目的，可以在每个系统上运行多次。

JASS 的基本功能特性包括：

支持绝大多数 Solaris OE 安全特性，预定义了 74 个固化功能和 14 个文件模板；

模块化和灵活的结构；

集成了直接文件复制功能；

高可配置性，使用变量来制定大多数特定内容；

有助于实施系统安全策略，包括初始固化,补丁/生命期管理

已经完成的 74 个功能包括如下几个方面：

- 禁止功能，禁止一些功能和服务；如Apache服务；
- 使能功能，使能一些功能和服务；如栈保护功能；
- 安装功能，安装特定部件，如安装sulog；
- 最小化功能，如最小化iPlanetWS;
- 打印功能，如打印jumpstart-environment；
- 移去功能，如移去unneeded-accounts；
- 设置功能，如设置user-password-reqs；
- 更新功能，如更新cron-log-size。

JASS 可以方便的进行客户化，使用了 40 多个动态和静态变量配置 JASS，以适应铁道部的安全策略要求和应用要求。

6.3.5.3咨询流程

此部分咨询服务包括以下工作：

1. 定义流程和步骤，以确保 Solaris 操作系统补丁得到及时更新
2. 定义流程和步骤，以便追踪和侦测铁道部关键业务服务器的安全漏洞
3. 固化 Solaris 操作系统，简化操作环境

   固化Solaris操作系统的咨询服务流程如下：

   - 审查当前服务器配置
   - 与铁道部IT员工访谈，获取安全性需求，包括：
   - 访问控制
   - 认证和授权
   - 保密
   - 获取服务器上应用和服务的需求和使用方式
   - 设计操作系统构造规范，包括建议的规程和处理
   - 为构造规范提供配置信息和文档变更
   - 按照构造规范实施服务器
   - 测试服务器实施
4. **提交 Solaris 安全性工具包 JASS 的源程序和相关文件，**传授相关知识。

所需咨询顾问及人天估计：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
安全顾问	1	12	1. 定义流程和步骤，以确保 Solaris 操作系统补丁得到及时更新 2. 定义流程和步骤，以便追踪和侦测铁道部关键业务服务器的	第一个点

			安全漏洞 3. 固化 Solaris 操作系统，简化操作环境 4. **提交 Solaris 安全性工具包 JASS 的源程序和相关文件，**传授相关知识。	
安全顾问	1	1		推广工程中的一个点

6.3.6 紧急响应体系

6.3.6.1内容提纲

虽然我们为铁道部采取了各种安全措施，减少系统的安全隐患，仍然可能会发生内部或外部的安全问题。Sun 认为应建立紧急事件响应体系，万一紧急事件发生了，可以增强铁道部的应急响应能力和应急响应流程。

6.3.6.2工具

在紧急响应体系中不需要工具。

6.3.6.3咨询流程

此部分咨询服务包括以下工作：

1. 确定铁道部关键资产和关键风险

Sun 公司将与铁道部一起，确定有价值的和机密的关键数据，明确何种事件可能损害

铁道部的关键资产，以及这些事件如何会发生。

2. 建立事件响应计划建议书

通过至多 3 次的访谈，并基于最佳实践，提交安全事件响应计划建议书，并在必要时举行 1 次研讨会。建议书的主要内容示例如下：

- 定义事件发生时的处理步骤
- 如何检测事件，如何确认安全事件
- 决定是否需要起诉
- 事件发生后需要首先完成的工作
- 建立事件响应队伍，定义队伍的责任和分工
- 如何恢复到事件发生前的状态
- 需要保留什么证物，如何保留证物
- 确定事件的紧急程度
- 评估已遭破坏数据的价值

所需咨询顾问及人天估计：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
安全顾问	1	12	1. 确定铁道部关键的资产和风险 3. 建立事件响应计划建议书 2.	第一个点
安全顾问	1	2	为其他点的实施，分析、评估和修订紧急事件响应计划，并进行统一的培训 （随后其他点的实施由铁道部负责）	推广工程中的一个点

6.3.7 日志系统与审计(Auditing and Logging)

6.3.7.1内容提纲

Sun 公司建议铁道部应设立一个审计追踪日志系统，审计服务器、防火墙和各种安全组件，同时建立日志管理策略。

6.3.7.2工具

Sun 建议采用第三方厂商的日志分析和审计产品。

6.3.7.3咨询流程

日志分析和审计的咨询服务包括以下工作：

1．建立日志分析和审计策略，策略的一些内容提纲如下：

- 日志分析和审计系统的部署；
- 日志分析和审计的查询、统计和报表规定；
- 日志分析和审计系统备份策略；
- 日志分析和审计文件的存储和备份策略；
- 日志检测的阈值设定，及相应处理规则；
- 日志警告的通知方式，7×24 小时的响应流程；
- 日志的分级分类；如调试信息、消息、警告、错误、严重错误；负载日志、事件日志、自我日志等。

2．审查日志分析和审计系统的管理策略符合性

所需咨询顾问及人天估计：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
安全顾问	1	3	1. 建立日志分析和审计策略； 2. 审查日志分析和审计系统的管理策略符合性	第一个点
安全顾问	1	2	分析、评估和修订日志和审计策略	推广工程中的一个点

6.3.8 安全策略的制定

6.3.8.1内容提纲

在安全策略咨询服务中，Sun 将提供铁道部员工建立安全策略的流程培训，并开发安全策略建议书。在咨询服务中，Sun 将和铁道部员工一起评估铁道部处理和运行环境，铁道部对安全性的期望，现有法律法规，契约和必须遵守的限制，已有的安全文档、流程、规程和当前及计划中的安全系统。Sun 将分析这些信息，并确定铁道部的安全需求，基于此开发符合铁道部特定需求的安全策略建议书。

咨询服务由知识传递，获得相关信息，安全策略建议书开发，提交安全策略建议书等内容构成。安全策略建议书将覆盖的基本领域包括：

- 信息管理
- 系统运行
- 系统完整性和控制
- 网络和通信
- 应用开发
- 入侵检测和事件处理
- 审计和监控
- 备份、储存和恢复

6.3.8.2咨询流程

安全策略的咨询服务包括以下工作：

1. 举行安全策略研讨会，向铁道部员工传授安全策略开发方法和流程；
2. 基于与关键人员至多 3 次的访谈，收集、分析、评估现有安全策略、安全需求及相关信息，包括：应用、系统和网络间的数据流以及信任和控制点；铁道部环境整体保密性、完整性、认证、授权、责任、可用性及保护级别的需求；确定适用铁道部的安全策略部件，其目标、边界、适用性和非适用性；目前安全性设施和加密设施的实施情况；关于信息备份、装入、存档、介质管理、储存、恢复的情况；入侵检测需求和事件处理等；
3. 建立基于上述需求信息的安全策略建议书；
4. 通过研讨会向铁道部提交安全策略建议书。

下面的安全策略建议书主要内容框架是一个示例：

- 数据的责任人、分类和安全性
    - 数据和资源访问
    - 口令使用
    - 加密的使用和密码管理
    - 网络安全性
    - 电子邮件的责任人、使用和运行安全要求
    - 安全事件报告流程
    - 安全事件响应流程
    - 监控和审计
    - 防火墙实施和管理
    - 病毒预防和保护
    - 终端用户责任和被认可的使用方式
    - 记录的储存和备份
    - 安全条例和教育

- 变更控制和配置管理

所需咨询顾问及人天估计：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
安全顾问	1	15	1. 举行安全策略研讨会，向铁道部员工传授安全策略开发方法和流程； 2. 基于与关键人员至多 3 次的访谈，收集、分析、评估现有安全策略、安全需求及相关信息 3. 建立基于上述需求信息的安全策略建议书； 4. 通过研讨会向铁道部提交安全策略建议书。	第一个点
安全顾问	1	2	分析、评估和修订安全策略	推广工程中的一个点

6.3.9 安全流程的制定

调查显示 IT 行业中 30%的安全失败都源于不安全的流程。基于 Sun 公司的经验和最佳实践，以及铁道部的具体情况，我们在以下方面完善完全流程：

1. 固化操作系统
2. 远程管理
3. Telnet 和 Ftp
4. 主权限（Root Privilege）

5. 远程访问和远程执行
6. Cron (Command Scheduling)
7. 基于主机的 TCP 访问控制
8. 审核检查
9. 网络文件系统
10. X Window 系统
11. 防火墙访问控制和配置
12. Web 服务器
13. 邮件服务器
14. 域名服务器
15. Cisco 路由器
16. 日志
17. 服务器备份
18. 配置管理
19. 漏洞扫描

所需咨询顾问及其工作内容：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
安全顾问	1	8	安全流程咨询服务	第一个点， 需要铁道部安全负责人参与
安全顾问	1	2	分析、评估和修订安全流程	推广工程中的一个点， 需要铁道部安全负责人参与

6.4 测试的服务内容描述

在系统集成测试阶段和用户验收测试阶段，Sun 的应用技术顾问和安全技术顾问会参与到测试工作中，与客户和第三方产品厂商和代理商一起进行测试。

所需咨询顾问及其工作内容：

顾问	*数量(人)*	*人天*	*工作内容*	*备注*
应用技术顾问	1	10	应用级的测试	第一个点
安全技术顾问	1	10	网络安全级的测试	
应用技术顾问	1	5	应用级的测试	推广工程中的一个点
安全技术顾问	1	2	网络安全级的测试	

7 项目实施规划

铁道部网络安全工程项目的涵盖范围为铁道部及所属路局、分局和站段等 63 个机关园区的网络安全建设。本工程项目需要实现的主要内容包括：

1. 网络安全管理与检测
   - 制定安全策略和安全流程
   - 防火墙的安装和部署
   - 针对关键服务器，进行 Solaris 操作系统的固化和漏洞检测
   - 建立网络病毒传播控制系统
   - 实现网络及网络安全设备的入侵检测和访问控制
   - 日志的定时收集和分析
   - 建立铁道部紧急响应体系
2. 完善应用服务和访问认证机制
   - 建立基于 PKI/CA 的铁道部数字证书系统。
   - 建立统一的用户管理、认证系统和分布式的授权系统。
   - 建立网络代理访问控制机制，对用户所有的访问进行策略控制和记录。
3. 实现与 INTERNET 动态物理隔离

为了实现上述内容在铁道部 63 个机关园区的网络安全工程建设，我们建议铁道部整体规划，分期分阶段进行工程项目的实施。

7.1 分期分阶段实施的建议

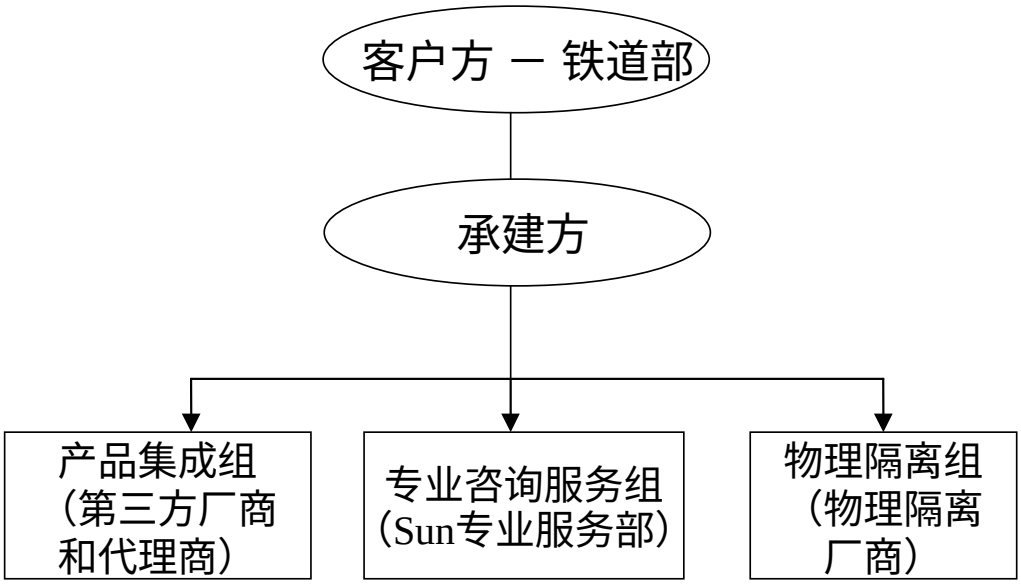
7.1.1 第一期试点工程度目标和实施范围

选出试点的机关园区，例如，广州路局的某分局。针对试点的分局，实现上述内容。在试点项目的实施阶段，分成试验阶段和生产环境的部署阶段。

7.1.2 第二期推进工程度目标和实施范围

第二期是针对其他路局进行工程推广。建议推进工程也是分阶段进行。

7.2 承建方项目组提供的服务内容



本项目中客户方是铁道部，承建方主要由下列三组构成：

1. 产品集成组：由相关的第三方厂商和代理商组成。负责相关硬软件产品的供货、安装、配置和售后服务

2. 物理隔离组：物理隔离厂商。负责物理隔离方案的实施和后期维护工作

3. 专业咨询服务组：由 Sun 专业咨询服务部提供。

7.2.1 Sun 提供的专业咨询服务

Sun 专业服务部提供的专业咨询服务包括：

1. 项目管理咨询服务

2. 应用集成咨询服务

3. 网络安全咨询服务

具体内容，请详见第六章《Sun 提供的咨询服务内容描述》。

7.2.2 产品的集成服务

在 Sun 安全咨询专家的指导下，依据 Sun 安全咨询专家设计的安全方案和相关安全策略与规范，本地系统集成商负责协调相关硬软件产品厂商和代理商，各硬软件产品代理商负责硬软件产品的供货、安装、配置和后期的产品维护工作。

7.2.3 物理隔离

由物理隔离厂商负责物理隔离方案的实施和后期维护工作。

Sun 首席安全设计师负责网络环境与物理隔离的接口方案的设计；物理隔离厂商负责物理隔离产品本身的实施和维护，和由于物理隔离系统所造成的网络环境故障的排除。

7.2.4 应用系统的改造

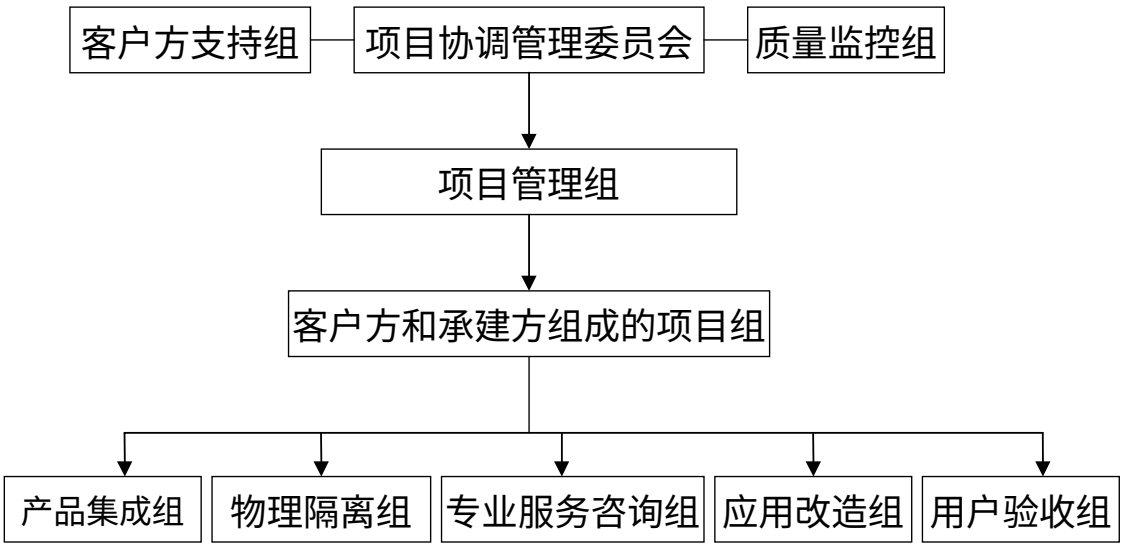
在 Sun 应用集成咨询专家的指导下，依据 Sun 应用集成咨询专家设计的应用集成方案和相关规范，铁道部应用改造组负责应用系统的改造和后期维护工作。

7.3 项目的组织架构

合理的、有效的项目组织架构的建立，为项目的成功实施提供了重要的保证。组织架构规范了项目实施过程中的责任和分工。当实施过程中问题出现时，能够尽快确定责任人，并且，当问题不能在责任人层次解决的，能够找到一条有效的渠道将问题尽快的解决。

7.3.1 建议项目的组织架构

Sun 建议铁道部网络安全项目的组织架构如下：



1. 项目协调管理委员会

- 组成成员

主要由各方的领导组成

- 组织职责

项目组织的最高决策和仲裁机构，负责对项目实施过程中的重大问题作出对项目合作各方均有约束力的决议，负责检查项目实施状况并听取项目经理对项目工作状况的汇报。

2. 项目管理组

- 组成成员

由各方项目经理组成：Sun 项目经理，客户方项目经理，本地系统集成商的项目经理等。

- 组织职责

项目管理的常务执行者；

负责项目实施过程中的各项管理、协调与组织工作；

负责制定项目计划，协调解决项目计划执行过程中出现的各种问题；

负责项目实施过程中的质量管理，颁布有关标准、制度与流程；

负责向项目协调管理委员会提交项目报告，并执行项目协调管理委员会作出的决议。

3. 产品集成组

- 组成成员：

由本地系统集成商领导，由各硬软件产品厂商和代理商组成。

- 组织职责

在 Sun 安全咨询专家的指导下，本地系统集成商负责协调相关硬软件产品厂商和代理商，各硬软件产品代理商负责硬软件产品的供货、安装、配置和后期的产品维护工作。

4. 物理隔离组

- 组成成员：

物理隔离产品的提供商

- 组织职责

负责物理隔离方案的实施和后期维护工作

5. 专业服务咨询组

- 组成成员：

Sun 专业服务部专家

- 组织职责 (请详见第六章：Sun 提供的咨询服务内容描述)

负责提供：

1) 项目管理的咨询服务

2) 安全咨询服务

安全架构设计、基础设施架构设计、安全策略制定、病毒防护、入侵检测、完整性检测等的咨询服务

3) 应用集成咨询服务：

应用集成中数字证书的使用、SSO、用户管理等的咨询服务

提供应用系统改造的总体方案和应用改造需遵循的规范，进行应用改造的技术指导，协助应用改造组制定应用改造计划

6. 应用改造组

- 组成成员：

由客户方的应用开发人员组成

- 组织职责

在 Sun 应用集成专家的指导下，应用改造组针对铁道部现有的应用系统进行改造、测试和后期的维护工作。

7. 用户验收测试组

- 组成成员

  由客户方的相关人员组成。

- 组织职责

  制定相应的业务操作和岗位流转的规范和制度；

  负责系统验收测试工作。

8. 质量监控组

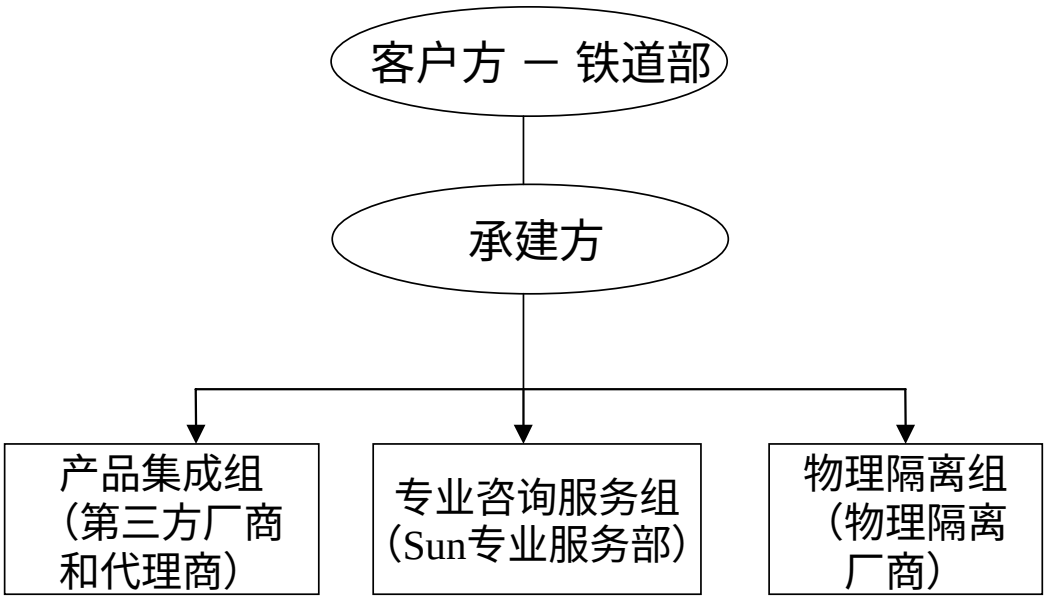
可以是客户聘请的第三方中立人员，也可以是客户方和承建方组成的一组人，专门负责项目实施的质量监控。

9. 客户方支持组

项目的实施会涉及到客户方一些其他部门，如：财务部门，安全部门，标准化部门，后勤部门，等等。这些部门的大力配合是项目顺利实施的关键。

7.3.2 承建方项目组的构成

承建方作为该项目的承包商。一旦合同签订，承建方将委派相应级别的人员参加本项目，包括技术人员和项目管理人员。



承建方成员：

角色	责任	来源	数量(人)
专业咨询服务组			
项目经理	负责对整个项目的项目管理提供咨询服务。负责 Sun 提供的服务的管理和协调工作。 制定和维护项目计划，进度安排，以及协调各方的项目资源。	Sun 项目经理	1
首席应用设计师（Chief Application Architect）	应用安全方面技术总负责人。 负责应用安全和应用集成关键的技术决策。从技术的角度同 Sun 的项目经理一起工作来评估进度、安排资源，确定关键的风险因素，领导应用系统整体技术框架的设计和实施。	Sun 首席设计师	1

应用集成设计师	和首席应用设计师共同进行应用系统集成方案的设计和应用改造规范的制定。负责和数字证书的使用、SSO、用户管理等相关的技术决策和技术问题的解决。	Sun 设计师	数人
首席安全设计师（Chief Security Architect）	网络安全方面技术总负责人。 负责网络安全关键的技术决策。从技术的角度同 Sun 的项目经理一起工作来评估进度和资源安排，确定关键的风险因素，领导网络安全系统整体技术框架的设计和实施。	Sun 首席设计师	1
安全设计师	和首席安全设计师共同进行系统框架的设计。负责安全架构设计、基础设施设计、安全策略制定、病毒防护、入侵检测、完整性检测等。	Sun 设计师	数人
产品集成组			
产品集成项目经理	负责协调相关厂商	本地系统集成商	1
各硬软件厂商和代理商	负责硬软件产品的供货、安装、配置和后期的产品维护工作。	- Sun 硬件 - Sun ONE 产品 - 外防火墙产品 - 日志产品 - 防病毒产品 - ooo	数人
物理隔离组			

物理隔离组	负责物理隔离方案的实施和后期维护工作	物理隔离产品的提供商	数人

7.3.3 建议客户方项目组的构成

建议客户方项目组的构成如下：

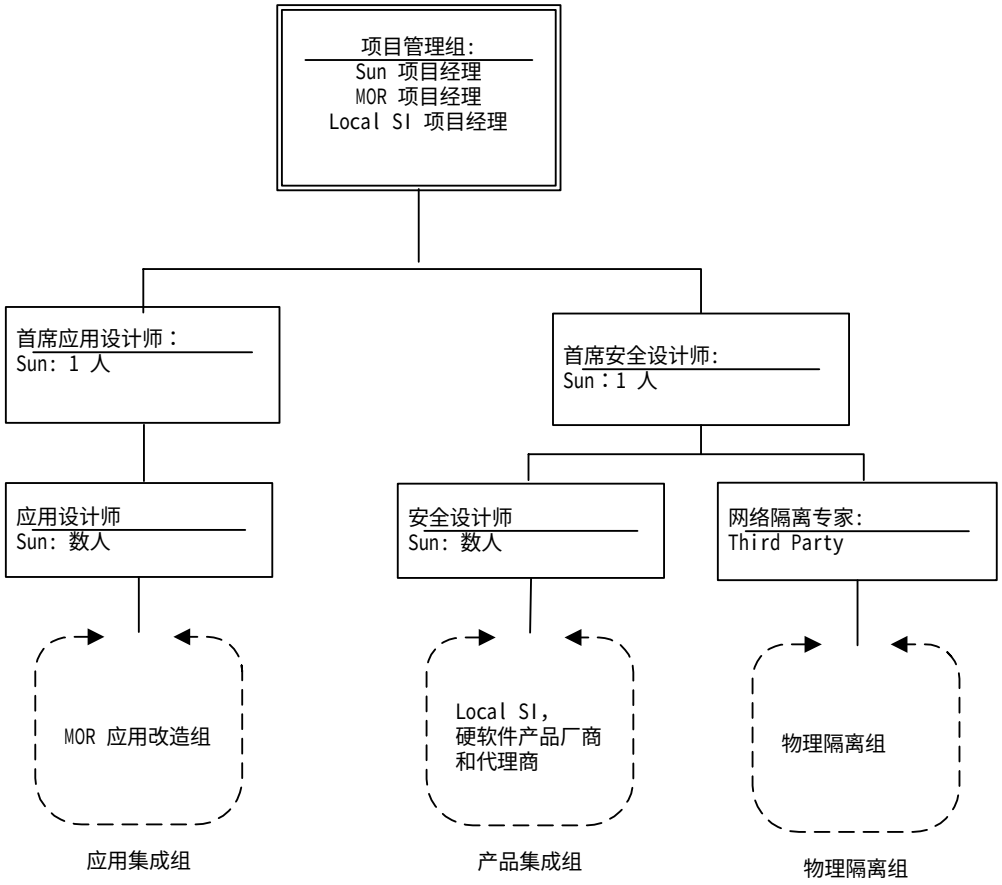
角色	**工作内容和责任**
项目领导	从其高级管理层中指定一名项目领导，领导项目协调管理委员会
项目经理	指定一名项目经理，参与项目的管理和客户方的协调工作
应用改造人员	在 Sun 应用设计师的指导下，负责铁道部应用系统的改造和后期的维护工作
用户验收测试人员	负责对整个系统进行验收

7.3.4 双方的责任和协同工作方式

项目实施各阶段		**承建方**	**客户方**
项目管理		**负责**	参与/**负责**
现状分析与评估		**负责**现状分析 制定现状评估报告	提供关于网络和应用的现状信息 参与讨论
产品集成	**安全咨询服务**	**负责 （Sun）**	协助
	产品供货、安装、配置和后期维护	**负责（Local SI 和硬软件厂商和代理商）**	协助
网络隔离方案的实施和后期维护		**负责 （Third Party）**	协助

应用集成	**应用集成的方案设计，规范制定**	**负责 （Sun）**	协助
	应用系统的改造和后期维护	协助	**负责**
系统集成测试		**负责**制定测试方案、计划，执行测试	参与制定测试方案、计划，参与测试
用户验收测试		参与制定测试方案	**负责**制定测试方案、计划，执行测试
系统试运行/上线		支持	**负责**

7.3.5 项目资源分配



	组成人员	工作内容
项目管理组	由 Sun 项目经理，铁道部项目经理和 Local SI 项目经理组成	负责整个项目的项目管理和协调。 制定和维护项目计划，进度安排，以及协调各方的项目资源。
应用集成组	Sun 首席应用设计师	应用安全方面技术总负责人。 负责应用安全和应用集成关键的技术决策。从技术的角度同 Sun 的项目经理一起工作来评估进度、安排资源，确定关键的风险因素，领导应用系统整体技术框架的设计和实施。
	Sun 应用设计师	和首席应用设计师共同进行应用系统集成方案的设计和应用改造规范的制定。负责和数字证书的使用、SSO、用户管理等相关的技术决策和技术问题的解决。
	铁道部应用改造队伍	在 Sun 应用设计师的指导下，负责铁道部现有的应用系统的改造，并负责应用系统的后期维护工作。
产品集成	Sun 首席安全设计师	网络安全方面技术总负责人。 负责网络安全关键的技术决策。从技术的角度同 Sun 的项目经理一起工作来评估进度和资源安排，确定关键的风险因素，领导网络安全系统整体技术框架的设计和实施。包括安全架构、基础设施设计、安全策略、病毒防护、入侵检测、完整性检测等。
	Sun 安全设计师	和首席安全设计师共同进行系统框架的设计。负责安全架构设计、基础设施设计、安全策略制定、病毒防护、入侵检测、完整性检测等。

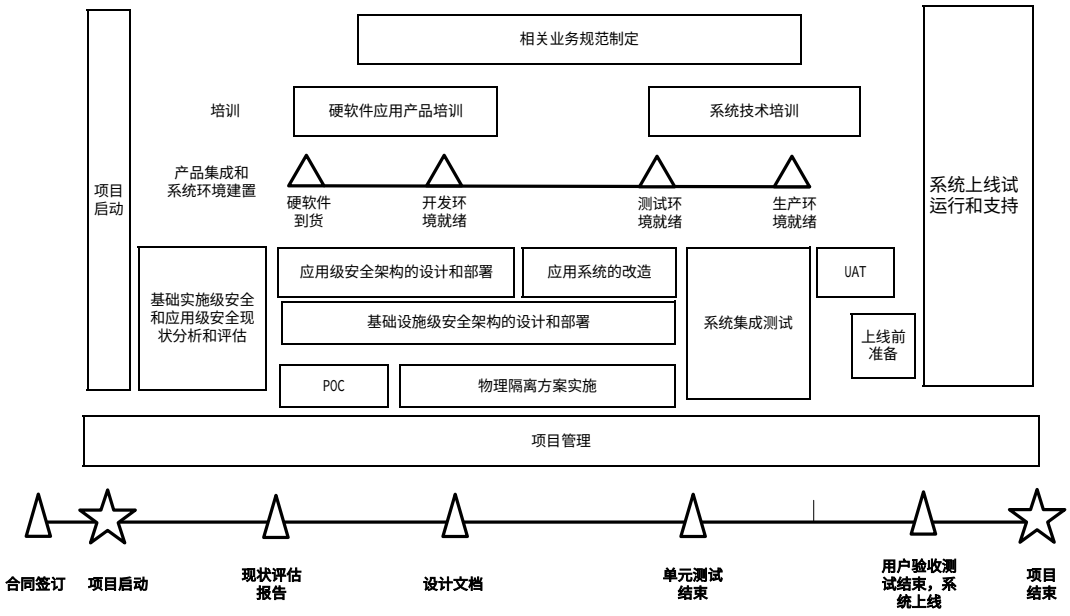
	Local SI 和下列硬软件厂商和代理商： - Sun 硬件 - Sun ONE 软件 - 外防火墙产品 - 日志产品 - 物理隔离产品 …	协调相关厂商，负责硬软件产品的供货、安装、配置和后期的产品维护工作。
物理隔离	物理隔离产品厂商	物理隔离产品的实施和后期维护。 Sun 首席安全设计师负责网络环境与物理隔离的接口方案的设计，物理隔离厂商负责物理隔离产品本身的实施和维护，负责由于物理隔离系统所造成的网络环境故障的排除。

7.4 项目实施计划

基于目前 Sun 对铁道部网络安全项目的了解，在本节中，Sun 给出了铁道部网络安全项目整体实施计划的初步建议。随着事情的进展和了解信息的增多，本项目计划需要进一步的细化。

1. Sun 建议的铁道部网络安全项目的整体实施计划

Sun 建议铁道部网络安全项目的整体实施计划如下图所示。



从整体上，Sun 建议项目的实施主体上分为以下各阶段：

项目启动：

在得到正式授权后，项目正式启动，召开项目启动会议。

现状分析和评估阶段：

针对铁道部基础实施级和应用级安全的现状，与铁道部相关人员进行交流，分析和评估。

安全架构的设计阶段：

针对铁道部对安全的需求，进行安全架构的整体设计。

安全架构的部署和应用程序的改造阶段：

基于设计方案，进行基础设施级和应用级安全架构的部署和应用系统的改造。

集成测试阶段：进行系统集成测试

用户验收阶段：进行用户验收测试，由铁道部的用户验收组负责。

系统上线：进行系统上线前的准备，将系统上线。

上线后的支持：上线后有一至两星期的热线支持阶段。

除了主体外，还有下述工作需要并行进行：

1．项目管理：贯穿整个项目的实施；

2．产品集成和系统环境建置：

需要进行开发环境、测试环境和生产环境的建置。

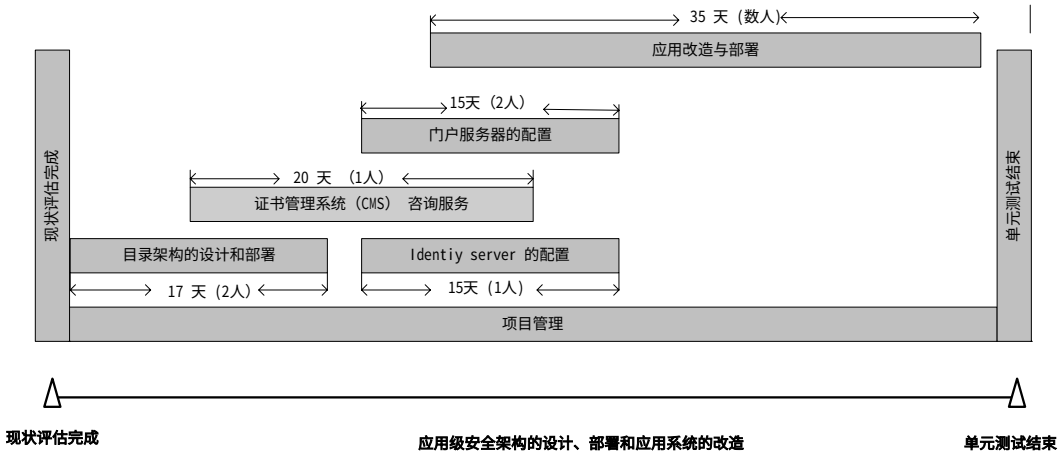
3．培训：产品相关的标准培训，与 PS 咨询服务相关的现场知识传授。

4．相关规范的制定

2. Sun 提供的应用级安全咨询服务的实施计划和相互依赖关系

关于 Sun 提供的应用级安全咨询服务，在设计和部署阶段，工作的安排和相互依赖关系如下：

应用级安全咨询服务的实施计划和相互依赖关系

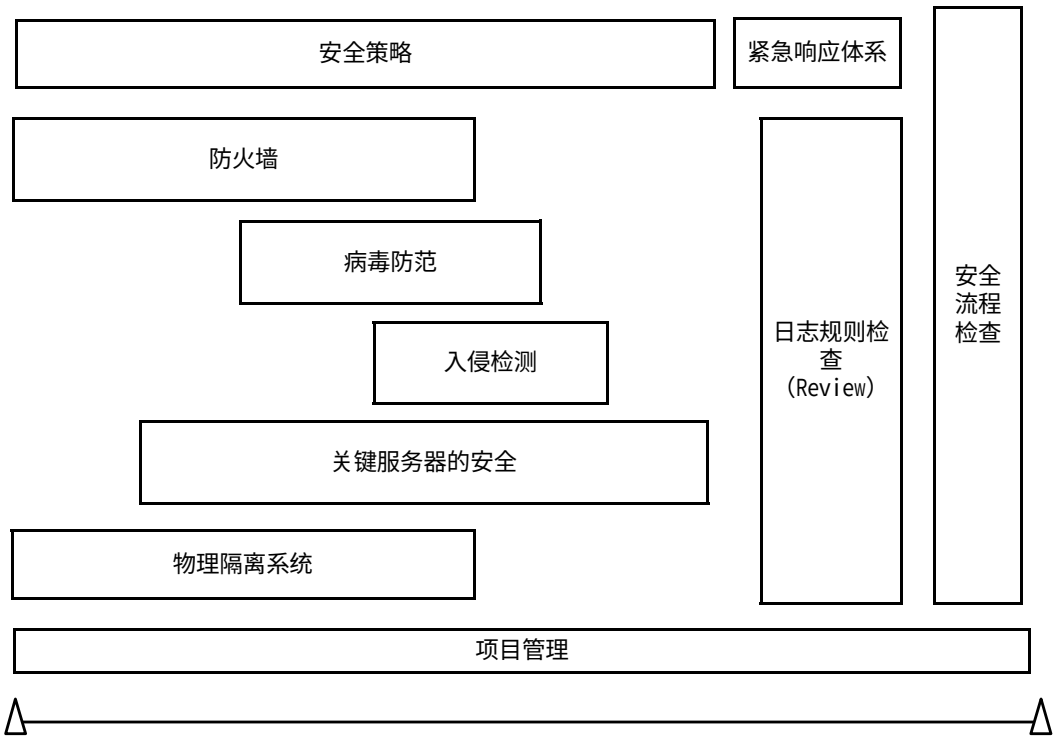


3. Sun 提供的基础设施级安全咨询服务的实施计划和相互依赖关系

关于 Sun 提供的基础设施级安全咨询服务，在设计和部署阶段，工作的安排和相互依

赖关系如下图所示。相关产品的安装和配置工作由相应的第三方厂商或代理商负责。例如，防火墙中，针对防火墙的方案设计和安全规则，Sun 负责检查核实（Review），防火墙厂商或代理商负责防火墙的安装和配置。

基础设施级安全咨询服务的实施计划和相互依赖关系



基础设施级安全架构的设计、部署

8 培训方案

Sun 公司针对铁道部的技术培训方案分两个主要部分：

1. Sun 公司标准的软件产品培训，包括 Solaris 和 Sun ONE 系列产品，为铁道部技术人员在项目开展过程前打下全面、扎实的技术基础。由 Sun 培训服务部提供。详见 8.1。

2. 在方案实施过程中针对 Sun 提供的专业咨询服务进行知识和技术的传授，使得铁道部技术人员在项目开展中获得实践知识，以便将来进行管理和维护。由提供咨询服务的 Sun 专业服务部提供。

8.1 Sun 培训部门的培训计划

8.1.1 概述

正如 Sun 公司始终着力发展网络事业，Sun 教育培训服务始终以人为本，着眼于其驾驭网络的能力。无论何种网络技术需要，Sun 公司都能为您提供培训解决方案。让我们提高您的技术技能，以达到专业要求。

通过提供员工完整的技能培训，帮助各个公司培训、吸收人才，在提高个人技能的同时也使公司事业获得发展。整个组织都从更高的专业技能，更新的操作质量及更高的系统效率中获益。

Sun 公司教育培训服务部在北京、上海、广州、成都设有 4 个培训中心，拥有一流的教学设备、经验丰富的专职教师为客户提供高质量的教育培训服务。

8.1.2 培训目的

通过此次 Sun 培训，使各路局的学员能够独立地进行系统管理、运行、故障处理、日常测试维护以及 Sun One Portal serve，Directory server，Certificate serve 的安装和配置等工作。

8.1.3 培训时间

为了提高培训效果，保证培训质量，Sun 公司将分三期进行培训。

期数	路局	人数	培训地点	天数	培训时间
第一期	13 个	13 人	Sun 北京培训中心	10 天	由铁道部同 Sun 公司共同商定
第二期	12 个	12 人	Sun 北京培训中心	10 天	由铁道部同 Sun 公司共同商定
第三期	25 个	25 人	通过 Internet 网上学习	90 天	由铁道部同 Sun 公司共同商定

8.1.4 培训课程

1、课程描述

本次培训课程主要介绍 Solaris8 System Administration, SunOne Portal server, SunOne directory server, SunOne certificate server, SunOne web proxy server，SunOne Identity server 核心概念和基本操作。

谁该参加：系统管理、维护工程师或相关工程师等。完成本课程后，学员将具备以下能力：

- 独立系统的安装，文件系统管理、系统备份，进程控制、用户管理、设备管理

- 网络环境下管理维护 Sun 的系统，NFS 配置和故障排除，并配置网络信息服务(NIS)环境
- 描述 SunOne Portal server 的基本功能，安装和配置 SunOne Portal server
- 描述 SunOne Directory server 的基本功能，安装和配置 SunOne directory server
- 描述 SunOne Certificate server 的基本功能，安装和配置 Certificate server
- 描述 SunOne Identity server 的基本功能，安装和配置 SunOne Identity server
- 描述 SunOne web proxy server 的基本功能
- 描述利用公有和私有秘钥进行加密通讯的原理

预备知识：

- 可成功地与 Solaris 系统进行交互
- 会使用 Vi 文本编辑器
- 与窗口系统进行交互
- 了解 internet

2、课程设置

培训级别	课程代码	课程名称	天数
V880/V480 系统培训	SA-238 SA-288	Solaris 8 系统管理 I Solaris 8 系统管理 II	5 天
Sun One 培训	PTL-2193 DIR-2217	Portal Server 3.0: 安装与配置 Directory Services: 分析与计划 5.X CMS, Policy server, 和 proxy 介绍	5 天
网上培训	DIR-1287-90	Directory Server 5.0: 安装与配置	90 天网上学

课程(Web)	DIR-1303-90	Identity Server 5.1: 安装与配置	习 90 天网上学习

8.1.5 师资情况

Sun 公司培训服务部在国内有四个培训中心，分别在北京、上海、广州、成都，全国共有十几位在相关专业经验丰富的培训教师。他们都具有多年的 UNIX 工作经验及教学经验，为各大公司及企业培养了数千名合格的系统管理员及开发人员。以下分别予以介绍：

姓名：严开明

简历：中国科学院软件所研究员，现为 SUN 北京培训中心专职教师，主要进行 Solaris 系统管理，网络管理，故障分析，性能管理等课程，以及硬件维护，安全性，存储设备管理等高级课程的培训。他在 SUN 的工作站上具有十余年的工作经验，七年的技术支持及培训经验。他技术精湛，培训经验丰富，深受学员的欢迎。

姓名：厉剑

简历：毕业于西安电子科技大学计算机系，现为 SUN 北京培训中心专职教师，主要进行 Java 编程，JavaBeans 组件开发，EJB，J2EE，以及 Solaris 系统管理，网络管理，存储设备管理等课程的培训。他在 SUN 的工作站上具有六年的技术支持，开发经验，四年的培训经验。曾为很多客户进行 Java 及 Solaris 的培训，如爱立信，摩托罗拉，华为，朗讯，香港电信，铁道部，平安保险等，受到学员的好评。

姓名：周东

简历：毕业于成都电子科技大学自动化系，现为 SUN 北京培训中心专职教师，主要进行 Sun One 产品系列课程，以及 Solaris 系统管理，网络管理，存储设备管理等课程的培训。他具有多年的 SUN，Netscape 和 CheckPoint 产品的技术支持及培训经验。曾为很多客户进行 Solaris 系统及 Sun One 产品的培训，如爱立信，摩托罗拉，朗讯，铁道部等，受到学员的好评。

姓名：王旭

简历：毕业于西安交大计算机系，现为 SUN 上海培训中心专职教师，主要进行 Solaris 系统管理，网络管理，故障分析，存储设备管理等课程的培训。她在 SUN 工作站上具有五年的开发及培训经验。曾为很多大客户进行 Solaris 系统的培训，如爱立信，摩托罗拉，朗讯，华为，上海贝尔等，受到学员的好评。

8.1.6 培训组织方式

- 铁道部负责培训的组织管理工作，Sun 公司将给予全力配合；
- Sun 公司负责提供准备培训场地、培训设备、培训资料、培训讲师等；
- 技术培训包括讲课及上机实验；
- 具体培训时间将铁道部和 Sun 公司共同商定。
- Sun 公司将对每个人员颁发毕业证书。

8.1.7 Sun 培训服务部

Sun 公司培训服务部（Sun Educational Services）是 Sun 公司提供专业培训的机构，是全球领先的培训解决方案供应商之一。Sun 培训服务部提供课堂培训、光盘培训、网上培训中心、专业认证课程、培训咨询服务和 Sun ELP(Enterprise Learning Platform)网上培训管理系统等完整的解决方案，可以满足不同客户的需求。培训服务部的服务内容包含电子商务、Java 技术、Sun 开发解决方案、Web 发布、Solaris 操作系统、网络与安全、硬件系统和服务器与存储等众多领域。目前，Sun 培训服务部在全球 60 个国家拥有 200 多个培训中心，每年培训学生人数超过 45 万，在用户中享有很高的声誉。

8.1.7.1为什么选择 Sun 教育培训服务？

- 经验丰富、信任可靠：19 年来，Sun 培训服务一直是您最好的技术培训来源。

- 优良的学习环境：我们所有的课程材料都是由业界专家设计，同时根据实际情况随时更新。
- 全球专业认证培训计划 :全球专业认证培训计划为系统管理员、网络管理员和 Java 程序员提供第三方认可的技能认证。
- 灵活变通：您可以根据个人需求选择多种培训方案。
- 便捷的现场培训：Sun 专家将应用您的设备对您进行现场指导。
- 自定义课程：Sun 培训服务咨询专家将和您一起确定您的培训内容，制定培训计划，设计培训课程以满足要求。
- 自学课程：Sun 培训服务借助多种媒体形式，提供九十多种自学培训课程。

8.1.7.2Sun 全球专业技术认证方案

在当今信息高速发展的社会中，人才决定了企业发展的基础。因此，如何评价员工的价值，或是个人如何证明自己的专业能力就成了关键。Sun 公司为了替业界建立一套认证的标准，特别针对最先进的科技，推出 Java 及 Solaris 技术认证方案。根据这些标准，企业可以此作为衡量员工技术水准的依据。Sun 公司推出的全球专业技术认证包括下列三种：

8.1.7.2.1 Java 认证考试

对于 Java 程序设计员，Sun 有两项认证：Java 程序员认证 Sun Certified Java Programmer(SCJP)和 Java 开发认证 Sun Certified Java Developer (SCJD)。SCJP 测验编程人员的 Java 程序设计概念能力，内容偏重于 Java 的语法及 JDK 的内容；SCJD 则进一步测试开发人员使用 Java 开发应用程序的能力，你必须首先完成一个程序设计的方案，再回答与此方案相关的一些问题。

8.1.7.2.2 Solaris 系统管理认证考试

对 Solaris/SunOS 系统管理员，Sun 推出系统管理认证 Certified Solaris

Administrator(CSA)。CSA 分为两个等级（Part I 和 Part II），分别测试使用着对 Solaris 系统管理的掌握程度。

8.1.7.2.3 Solaris 网络管理认证考试

为了测试使用着对于 Solaris 网络管理能力，Sun 推出了网络管理认证 Certified Network Administrator(CNA)。内容包括基本网络概念 ,Routing and Subnet, Security, Performance Tuning , DNS，DHCP 等。

8.2 Sun 专业服务部门的培训计划

本节描述的是，在方案实施过程中针对 Sun 提供的专业咨询服务进行知识和技术的传授，使得铁道部技术人员在项目开展中获得实践知识，以便将来进行管理和维护。这部分培训是由提供咨询服务的 Sun 专业服务部提供。

8.2.1 培训目的

通过方案实施过程中知识传授的培训，使各 IT 职能部门人员掌握提供咨询服务的各部分并接管，并对将来的管理和升级负责。

8.2.2 培训师资

由提供咨询服务的专业人员担任培训讲师。

8.2.3 培训组织形式

由于本部分的目的是掌握方案的实践知识，因此在项目开展中接受相关知识是最好的学习方式。

因此要求在咨询服务过程中，铁道部配备相应技能的技术人员参与项目的实施。在项

目实施过程之中，与 Sun 的咨询专家一起参与方案的讨论、确定和实施，通过日常实际动手操作，在实践中掌握相关技能；

8.2.4 培训费用

包含在 Sun 专业咨询服务的报价体系之中。

8.2.5 培训内容

1、统一用户管理知识传授

通过用户管理和目录结构设计咨询服务，我们帮助铁道部建立统一的目录系统，保存和管理包括公开密钥在内的用户身份认证信息。知识传授的内容包括：

- 用户目录信息的树形结构介绍（Directory Information Tree）
- 用户目录结构属性的设置介绍（Schema）
- 用户管理流程介绍

2、认证管理系统（CMS）知识传授

通过 CMS 咨询服务，我们帮助铁道部将现有的 CMS 系统升级到最新版本，并建立适当的 PKI 管理流程和体系架构。知识传授的内容包括：

- 证书发放流程介绍
- 用户注册授权规范和 CMS 体系架构介绍
- CMS 系统管理介绍

3、门户技术咨询服务

通过门户技术咨询服务，帮助铁道部集成 Web 和某类 TCP/IP 应用程序，并在这些内容之间提供单点登录（SSO）功能。知识传授的内容包括：

- 门户架构介绍

- 门户服务器部署介绍
- 门户频道开发经验介绍

4、应用改造的咨询服务

通过应用改造的咨询服务，帮助铁道部建立基于 PKI 的集中式应用授权系统并实现 SSO 功能。知识传授的内容包括：

- SSO 方案设计介绍
- C/S 应用程序上 SSO Web Agent 的设计、开发内容介绍
- C/S 应用程序上客户端应用改造步骤的制定和指导
- C/S 应用程序上服务器端应用改造步骤的制定和指导
- 编码规范的制定和指导

5、入侵检测工具安装配置

通过入侵检测工具的安装、配置和入侵检测的实施，帮助铁道部建立入侵检测功能。知识传授的内容包括：

- 入侵检测工具的安装和配置
- 入侵检测工具的日常使用
- 入侵检测报告的编写

6、完整性保证工具安装配置

通过完整性保证工具的安装、配置的实施，帮助铁道部建立系统完整性保证功能。知识传授的内容包括：

- 完整性保证工具的安装和配置
- 完整性保证工具的日常使用
- 系统完整性报告的编写

7、Solaris 系统安全性强化知识传授

通过系统安全性强化工具的安装、配置和系统安全性强化的实施，帮助铁道部建立系统安全性强化功能。知识传授的内容包括：

- 系统安全性强化工具的安装、配置
- 系统安全性强化工具的使用
- 系统安全性强化工作流程

8、安全策略开发流程知识传授

通过系安全策略开发，帮助铁道部建立企业安全策略。知识传授的内容包括：

- 企业安全策略评估流程
- 企业安全策略开发流程
- 企业安全策略的维护
- 企业安全策略的部署

9 服务支持体系

9.1 项目背景

铁路运输管理系统网络安全项目需要建立全国铁路系统安全生产网的纵深安全体系，将要为铁道部所属各路局、分局采购内部网络访问控制系统平台硬件、外部网络访问控制系统平台硬件以及构成纵深安全体系所需要的相关软件产品。

为配合此次铁道部铁路运输管理系统网络安全项目设备招标项目的要求，太阳计算机系统公司（以下简称 SUN 公司）将参与服务器及存储平台和 Sun 公司满足本项目招标需求的有关软件产品的投标，并提供相应的技术服务。在认真分析本次招标要求和系统运行要求的基础上，编写本专业服务支持方案。我们的目标是：为本项目提供最先进的高性能服务器平台和专业高效的系统支持服务，保证系统在运行生命周期内具有最高的系统可用性和最合理的系统总拥有成本。

SUN 公司在投标的服务器平台和服务支持计划中，我们始终坚持如下原则：提供整体的解决方案，配合铁道部成功完成本项目。

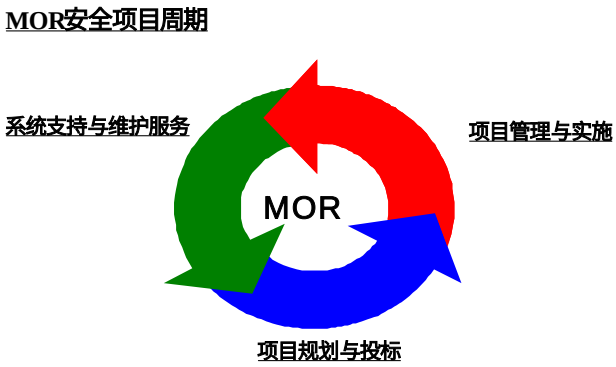
9.2 SUN 公司服务理念

SUN 公司的服务理念是为铁道部铁路运输管理系统网络安全项目提供基于系统生命周期内最全面的专业服务，特别在此项目从规划投标，项目实施到系统维护支持提供全程服务，并且保证系统具有最高的系统可用性和最合理的系统总拥有成本。SUN 公司将凭借全球领先的 UNIX 系统的技术优势和成功的专业服务经验，高效的服务体系为本项目提供最高质量的服务。为此，SUN 公司已经组成专门化的项目团队来配合此项目的实施。

9.3 技术支持服务阶段

铁路运输管理系统网络安全项目周期将包括三个主要阶段：

- ✧ 项目规划与招标、投标阶段
- ✧ 项目管理与实施阶段
- ✧ 系统支持与维护阶段



Sun 公司技术支持服务集中在：

- ✧ 项目管理与实施阶段—提供项目实施服务
- ✧ 系统支持与维护阶段—提供支持与维护服务

在铁道部计算中心与 Sun 公司授权代理签订设备采购合同，以及与 Sun 公司签定售后服务合同后，项目进入工程实施阶段。

在系统完成验收测试以后，整个系统的运行进入保修期，即进入系统支持与维护阶段。系统的维护及技术支持是系统集成的一个重要方面，体现了总体解决方案的质量。Sun 公司有着完整的技术支持与服务体系，在全国拥有众多的技术服务机构，保证能为系统的维护提供优质的服务。

9.4 项目实施服务

9.4.1 项目实施服务内容

在本项目中，Sun 公司将提供铁路运输管理系统网络安全项目所需要的硬件产品和相关 Sun ONE 软件产品，包括：

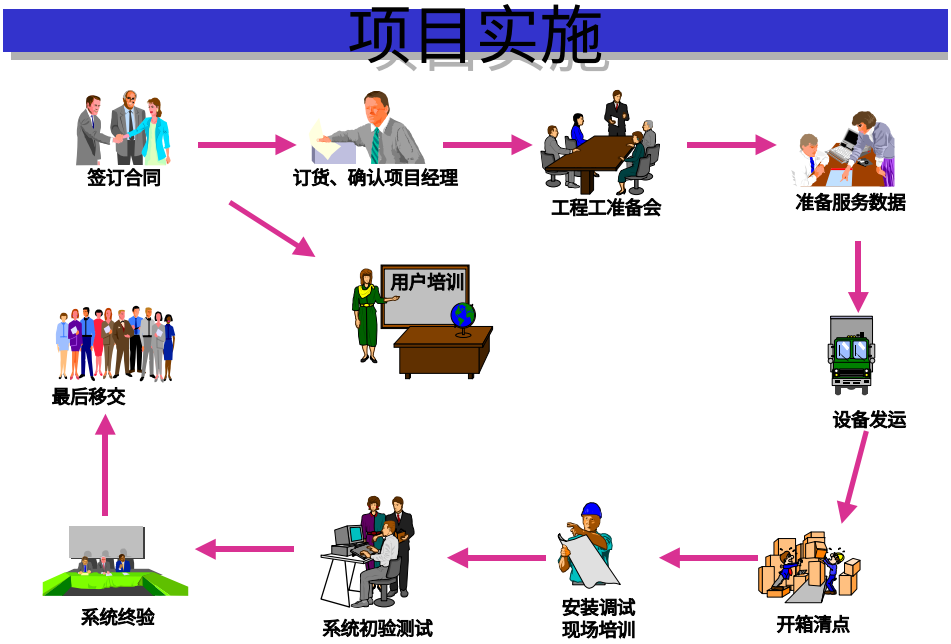
- 内部网络 A 类访问控制系统平台硬件
- 内部网络 B 类访问控制系统平台硬件
- 外部网络访问控制系统平台硬件
- 访问控制系统软件
- 数字证书注册代理软件
- 授权管理软件

9.4.2 项目实施服务流程

项目实施主要分为三大步骤，即：签订合同、工程实施的准备以及工程实施。

- 签订合同是项目实施的开始，是双方承诺的责任和义务以法律形式确定下来的时刻。
- 工程实施的准备是投标商与供货商在紧密配合下完成设备订货、生产、发货、运输与供货的过程，同时也包括了对用户的先期培训。
- 工程实施是投标商与供货商以及最终用户在紧密配合共同完成设备的到货、初验、安装、调试与验收的过程。

项目实施的流程如下图所示：



9.4.3 设备到货前支持

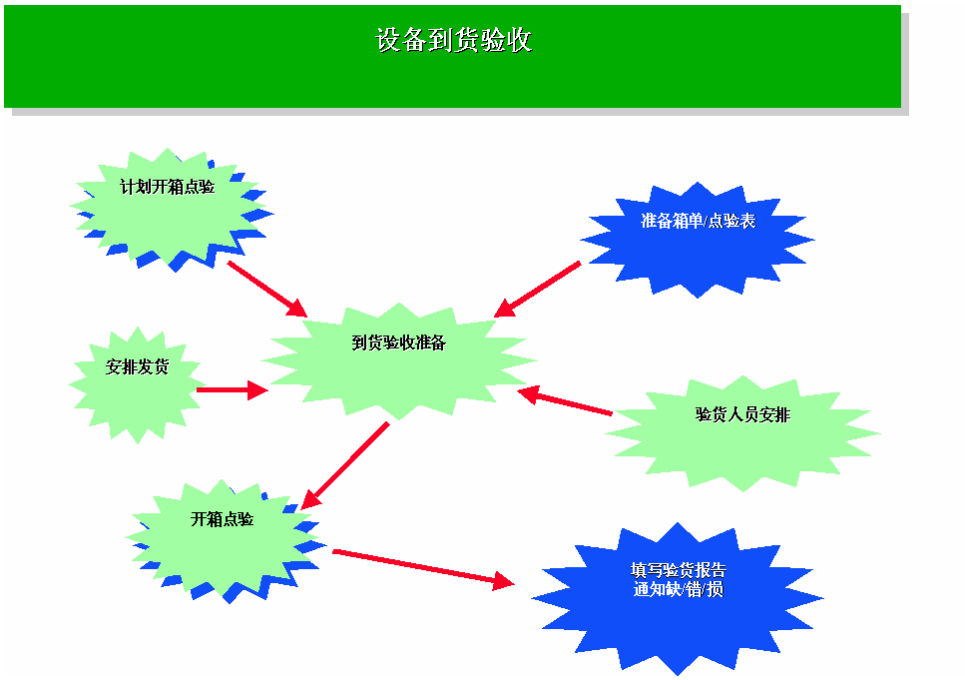
在 Sun 公司工厂进行设备生产的同时，Sun 公司企业服务部门的专业人员将与铁道部铁路运输管理系统网络安全项目的相关人员协商确定设备的安装方案，场地要求。这项工作一般在到货前两周开始进行。Sun 公司的专业服务人员将根据不同铁路局、分局的机房的实际情况制定详细的场地需求，以配合用户在计划的时间内使机房场地符合安装要求。

同时，Sun 公司专业服务人员将向铁道部铁路运输管理系统网络安全项目组提供具体的安装计划和相关问题的技术解决方案，并提供详细的文档备案。

9.4.4 系统到货、安装与设备初验

9.4.4.1设备到货与初始验收

设备到货验收的过程如下图：



设备到货清点验收并完成了系统软件硬件的设备调试后，Sun 公司实施工程师将与供货代理商一起，配合用户技术人员以及有关方面进行设备集成的初始验收，其中包括服务器设备、系统软件、配套设备和协助用户安装的基本应用软件。

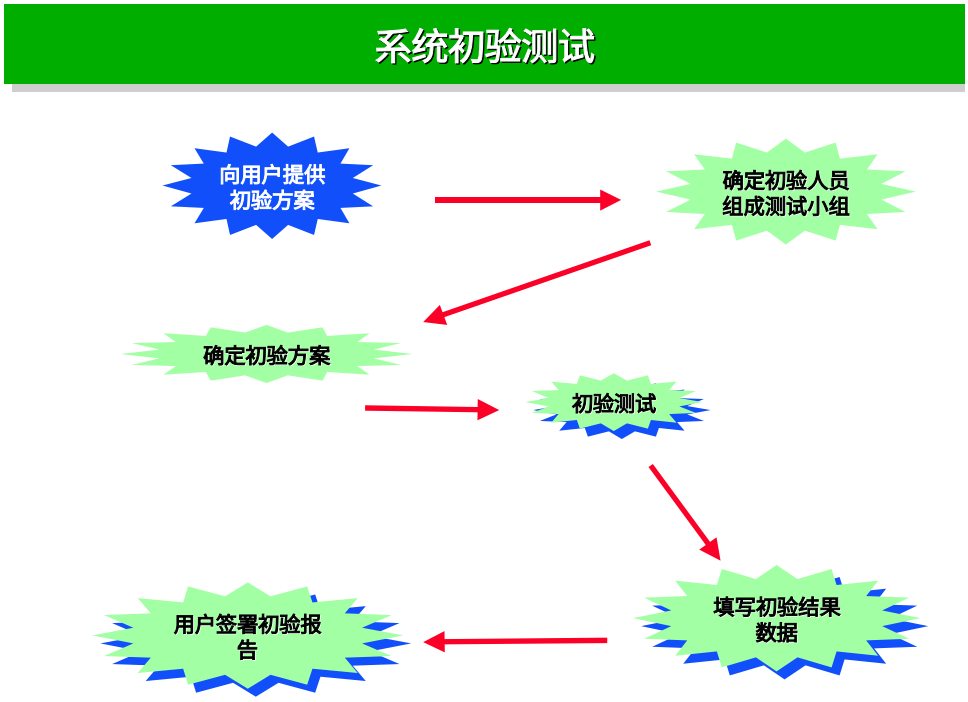
设备初始验收的主要内容如下：

1. 设备到货后与项目单位一起共同配合商检部门进行开箱检查，当出现损坏、数量不全或产品不对等任何问题时，均由供货方负责及时解决。

2. 在到货验收时将依招标文件要求进行，对全部设备的型号、规格、数量、外型、包装及资料、文件（如装箱单、保修单、随箱介质等）的验收。

3. 按标书技术部分要求对产品的配置进行测试检查，并做出测试方案和测试报告。
4. 与配套设备进行连接测试，构成相应的硬件平台、软件平台。
5. 实现所有硬件设备在标书指定的地点和环境下实现正常运行。

设备初始测试的流程如下图：



9.4.4.2 服务器设备的初验步骤

- 检查产品的外型和包装；
- 检查产品型号和产地；
- 检查服务器的基本配置是否正确并与合同中设备规格相符；
- 检查文档资料是否齐全，包括装箱单、保修单、随箱介质和文档等；
- 检查连接用各种线缆和电源线是否短缺，是否接口有误；

- 系统集成工程师负责将计算机的各个模块组装在一起；
- 进行产品性能测试和检查，测试机构能够提供性能指标的不再进行测试，以测试机构的数据为准。
- 连接电源，打开计算机进行加电测试，对无法加电的模块设法查找出故障原因。要求：
    - 计算机的各个模块都能加电。
    - 计算机的各个指示灯指示正确。
    - 系统能够通过加电时的检测。
    - 系统能够检测出已安装的外设和内设。

9.4.4.3软件的验收

软件的验收包括以下几个方面：

- 软件载体和文档资料的验收；
- 软件许可证的验收；（Sun ONE 软件许可证的验收只限于铁道部信息中心北京总部 ）

以上所有内容必须和软件订购合同相符。

9.4.4.4设备安装及调试

Sun 公司将为本项目提供系统的安装与调试服务，包括 Sun 公司硬件、Solaris 操作系统。

Sun 公司将为本项目提供系统的安装与调试服务，包括 Sun 公司硬件、Solaris 操作系统、及相关 SUN 公司产品。

实施前：

- 为本项目提供最优化的维护服务支持方案。

- 专门化的项目小组，认真分析项目需求。
- 全面的方案论证及优化，保证项目成功实施。

中标后，SUN 公司将根据双方确定的工程计划，按时完成设备安装调试工作。为了减少意外事故的发生，将采取以下安装、调试流程作为每个系统的安装标准步骤：

1. 按照装箱单清点货物
2. 安装硬件（服务器、管理控制工作站）
3. 安装系统外设（光驱、磁带库和磁盘阵列）
4. 连接终端集线器及网络集线器
5. 设置主机名
6. 设置网络地址
7. 配置系统内核（Configure Kernel）
8. 安装并配置系统并行管理软件
9. 设置服务器用户名，用户组及用户宿主目录
10. 安装服务器及磁盘阵列管理软件
11. 安装其它软件包
12. 安装随机手册
13. 填写安装报告
14. 测试验收

Sun 公司服务部将在用户配合下承担本项目中 Sun 公司硬件平台的安装与调试任务。包括：服务器系统、磁盘阵列等。具体步骤及内容如下 ：

- **服务器安装：**

- 复查安装地点准备情况
  - ✓ 在编制系统安装计划前安装地点环境及安装所需条件（如电源 、插座及空调等）

- 硬件设备核查及安装
  - ✓ 查对装箱单确保所有零部件与装箱单相符
  - ✓ 安装内外部件如内存 、 硬盘和 PCI 卡
  - ✓ 设置 SCSI 设备如硬盘 、 磁带和 CD-ROM 驱动器，DVD-ROM 等
  - ✓ 开电源并测试所有硬件设备
- 安装 Solaris 操作系统
  - ✓ 根据用户应用系统并考虑未来使用对文件系统和交换设备的需求为硬盘分区
  - ✓ 安装操作系统并根据需要将其配置成NFS文件服务器 ，且/ 或无盘客 户启动服务器
  - ✓ 配置系统主机名 、 IP 地 址 、 NIS/NIS+、 域 (Domain) 等
  - ✓ 如需要为无盘客户配置其他文件系统类型
- 后续配置及客户化
  - ✓ 客户网络配置
  - ✓ 设置 UNIX 标准电子邮件主机 ， 缺省路由
  - ✓ 定义 、设置并测试自动 Mount 的文件系统
  - ✓ 配置 DNS
  - ✓ 设置用户(User) 帐号 、用户组(Group) 以工作目录(Home Directory)
- 现场演示

- ✓ 系统加电、系统启动和系统关闭 (Shut Down)
- ✓ NIS/NIS+ 管理
- ✓ 如果需要，介绍 OpenWindows
- ✓ 介绍 PROM 工具

➢ 安装报告与验收

- ✓ 详细记录系统安装信息， 并留给用户一份存档

Sun 磁盘阵列安装:

➢ 安装前准备

- ✓ 安装地点准备情况询问
- ✓ Sun 磁盘阵列体系结构技术资料
- ✓ 制定安装计划

➢ 安装前现场勘察

- ✓ 检查现有或已采购的设备
- ✓ 与客户讨论 RAID 特性
- ✓ 讨论 Sun StorEdge D2 storage 磁盘阵列的硬件特性

➢ 磁盘阵列安装

- ✓ 安装磁盘阵列
- ✓ 安装 Sun 磁盘阵列的系统补丁(Patch)
- ✓ 安装 Sun 磁盘阵列软件及其补丁(Patch)
- ✓ 启动 GUI 界面
- ✓ 配置磁盘阵列

Sun ONE 软件安装内容 （参见软件安装计划）

Sun ONE 软件安装将由公司指定的授权合作伙伴完成.

1、SUNONE 软件安装的主要工作内容：

- ◆ 确认系统需求(硬件环境、网络环境、操作系统版本和所安装产品的版本)
- ◆ 确定产品之间的层次和相互关系，确定各个组成部分部署情况和安装路径
- ◆ 确定产品安装类型和必要信息，如是否使用当前的目录服务等
- ◆ 将安装和配置的参数纪录到如下的软件安装核对表中

2、 SUNONE 软件安装验收标准

- ◆ 各项服务能正常启动
- ◆ 软件安装符合配置参数的要求
- ◆ 完成下表规定的各项安装工作

参 数	说 明	参考值
硬件配置	硬件配置	
操作系统版本和补丁号	操作系统版本和补丁号	System version Example: solaris 8 Patch number Example:
产品安装路径	安装程序的路径： 来自安装 CD 盘或 iPlanet Web 站点	Example: `/usr/temp/msg51opt` *install-binaries:*_____

目录服务器的管理员 DN	安装： 目录管理员的设置	**Directory Manager DN** Example (default): `cn=Directory Manager` **Password**: `iPlAnEt1` **Directory Manager DN**: _____ **Password**: _____
目录服务器的标识、端口和后缀	软件安装： 目录服务器的设置	**Server Identifier** Example: `budgie` **Server Port** Example: 389 (default) **User Suffix** Example: `o=siroe.com` **Server Identifier** _____ **Port** _____ **Suffix**_____
目录服务器的组织名称	目录服务器的组织名称	**Organization Name** Example: `o=siroe.com` **Organization Name**
目录服务器的主机名称和域名	软件安装： 目录服务器的设置	**Host and Domain Name** Example:`budgie.siroe.com` **Host Name Identifier** _____
管理服务器的管理端口	软件安装： 指定管理端口	**Administration Port** Example: `5000` **Administration Port Number**: _____
服务器所需的邮件服务器信息	服务器所需的邮件服务器信息	**POP3 Server**: pop3..`siroe.com` **SMTP Server**: smpt.`siroe.com` **Webport:** `80` **POP3 Server**: _____

		SMTP Server: _____ **Webport:** _____
服务器完整的主机名	服务器的主机名和域名	**Fully qualified** example: `budgie.siroe.com` Host example: `budgie` Domain example: `siroe.com` **Server Fully Qualified Host Name**: _____
管理服务器	管理服务器的管理员和密码	User example (default): `Admin` Password example: `iPlAnEt1` **Server Services User:** _____ **Password:** _____
代理管理工具运行于 Web 服务器的端口号	为管理服务器安装的代理管理工具，确定运行于那个端口	**Delegated Administration Host** and Port example: **Host Name**: `budgie.siroe.com` **Port**: `8080` (default) **Delegated Administration Host Name**: _____ **Port Number**: _____
Web 服务器管理端口号	代理管理工具所需的 Web服务器管理端口号	**Administration Server Port for Web Server** Example: `8000` **Administration Server Port for Web Server**: Port Number:_____

Web 服务器配置路径	代理管理工具所需的Web服务器的路径	Example: `/usr/netscape/server4/https-budgie/config` **Directory**:_____

注：此表为 SUNONE 软件安装的标准工作列表，在 SUNONE 系列软件中根据软件不同工作列表有所不同。

9.4.5 系统验收

系统的测试及验收建议按照 Sun Solaris VTS 的验收程序而进行。Sun 产品之系统验收包括所有 Sun 的硬件产品、操作系统及非捆绑软件安装之验收。在所有 Sun 的硬件产品及操作系统安装完毕后，运行诊断程序 sunvts 进行硬件测试，若三次系统测试无错误，则系统验收通过。

《系统安装、测试、验收报告》样本

一、所有硬件无遗漏并且工作正常	检查安装系统，确保所有所用部件无遗漏并且工作正常。	□ 通过 □ 未通过
二、安装标准	1. 物理检查安装系统，确保所有部件正常工作。 2. 针对安装要求，确保硬件安装条件正常。 3. 确保所有硬软件都已被记录在维修合同中。	□ 通过 □ 未通过
三、硬件检查	**1 基本检查（电源、系统板、以及内存）** 1] 、参照系统管理员手册关闭系统 2] 、使用系统 OBP 中提供之 POST 命令检查系统，步骤如下： ⇒ 开机 ⇒ 系统出现公司标志及提示信息后同时键入 STOP 键和 A 键，以便使系统进入 OK 状态。 ⇒ 运机 OBP 命令 setenv diag-switch? True ⇒ 运行 OBP 命令 reset ⇒ 系统出现公司标志及提示信息后同时键入 STOP 和 A 键，使系统进入 OK 状态。 3] 、将一个哑终端连接到系统的 ttya	□ 通过 □ 未通过

	上，或者如果没有哑终端时，将串行线的另一端连接到另外一台 Sun 计算机的 a 或 b 口上，修改 / etc / remote 文件，通过使用 tip 命 令将该 Sun 计算机仿真成一个哑终端 4] 、将被测试计算机系统开机。对于服务器，将它前端的钥匙放在诊断位置上。 5] 、此时在哑终端上，系统会打印出所有诊断结果，检查该结果并确保没有任何错误信息。 **2、 磁盘诊断** 1] 、使用 root 登录。 2] 、运行 format。 3] 、对于系统中的所有磁盘，运行以下命令 ⇒ 选择要被检查之磁盘 ⇒ 选择 analyze 菜单 ⇒ 对于非系统启动盘使用 test 菜单，如果是系统磁盘则选择 read 菜单 ⇒ 键入 yes 进行检查 ⇒ 确保没有任何错误信息出现 **3、 磁带库诊断**	□ 通过 □ 未通过

	1] 、使用 root 登录 2] 、将一个空白磁带放入磁带库中 3] 、运行命令 mt –f 〈磁带库名〉start 4] 、运行命令 mt cvf 〈磁带库名〉 ./etc/* 5] 、运行命令 mt –f 〈磁带库名〉 rew 6] 、运行命令 tar tvf 〈磁带库名〉 7] 、运行命令 cd /tmp; tar xvf 〈磁带库〉 8] 、确保以上步骤无任何错误信息 **4、 光盘驱动器诊断(** 1] 、使用 root 登录 2] 、将一个 CD 放入光盘驱动器中 3] 、确保 CD 中所有内容可被读写并无任何错误发生 **5、 软盘机诊断** 1] 、使用 root 登录 2] 、放一张空软盘到软驱中	□ 通过 □ 未通过 □ 通过 □ 未通过

	3] 、运行命令 fdformat 或 fdformat –U 格式优化 软盘 4] 、启动文件管理器应用程序，并从它的 File 菜单中选择运行“ open floppy ” 5] 、确保数据文件可以拷入/拷出软盘 并无任何错误	□ 通过 □ 未通过
四、软件验证	**1、操作系统** 1] 、检查所有要求的操作系统及其相关增强软件都已正确安装 2] 、确保所有磁盘已按用户要求进行了正确分区 3] 、检查所有文件系统已按用户要求进行了正确的设置 **2、网络系统** 1] 、确保系统中的每个网卡接口都已进行了正确的设置 2] 、配合进行整个网络系统的路由信息设置，从而 ping 可被成功地操作 3] 、进行 Telnet、ftp 等的网络测试 **3、磁盘影像** 检查磁盘阵列已按用户要求正确完 成了 Raid 0、Raid 1、Raid 5 配置	□ 通过 □ 未通过 □ 通过 □ 未通过

	4、非操作系统软件 检查所有非操作系统软件已按安装手册步骤 正确地完成安装（只是安装，不包括设置）	□ 通过 □ 未通过 □ 通过 □ 未通过
五、支持就绪	1、记录系统所有信息，确保 Sun 公司工程师可以方便地对系统进行维护 2、确保用户拥有所有相关资料，以便在系统出现问题时，用户方便准确地与 Sun 公司联系。	□ 通过 □ 未通过

9.4.6 文档计划

技术文档提交

在系统安装和验收过程中，Sun 公司将向用户提供一系列的技术文档。

- 系统安装规划

  在系统实施前向用户提供系统安装规划并由用户认可。

- 培训计划 （参见培训计划）

  在培训前，向用户项目负责人提供培训计划，包括培训地点、时间、讲师、课程、教材、食宿和人数安排等并得到用户的认可。

- 实施和安装计划

  在实施前向用户提供系统实施和安装计划。

- 安装，测试及验收

Sun 公司将提供设备安装，设备测试的详细方案及测试内容。项目结束时 SUN 公司将提供所有系统安装报告并提交给项目单位。

9.5 Sun 公司系统支持与维护服务

在系统完成验收测试以后，整个系统的运行进入保修期，即进入系统支持与维护服务阶段。系统的维护及技术支持是系统集成的一个重要方面，体现了总体解决方案的质量。Sun 公司有着完整的技术支持与服务体系，在全国拥有众多的技术服务机构，保证能为系统的维护提供优质的服务。

Sun 公司将为本项目提供 3 年的系统支持与维护服务，包括全部 SUN 公司硬件产品及相关软件。具体内容请参见 9.5.2. 保修期过后 Sun 公司将用户协商并在签订继续服务协议后提供服务。

9.5.1 服务目标

- 提供快速高效，最高质量的服务， 目标最大化客户系统的可用性
- 提供系统生命周期内的支持服务
- 主动及高优先性服务
- 最低的系统可拥有成本

9.5.2 服务计划要点

- ✧ **7x24x365 在线支持数据库**
- ✧ **7x24x365 电话支持**
- ✧ **SUN 硬件产品工作日 5x8 小时现场支持**
- ✧ **SUN 多厂商支持计划**
- ✧ **SUN 在线支持中心**
- ✧ **可提供系统远程实时监控支持及故障诊断**
- ✧ **主动预防式的支持模式**
- ✧ **高优先性的响应支持**

9.5.3 系统支持与维护服务内容及范围

全方位支持

针对各个系统安装地点：电话支持包括对软件， 硬件和网络应用方面的支持。软件电话支持包括对 Sun 操作系统和经 Sun 公司发放许可证的其它非随机软件的支持。硬件支持包括将系统恢复到正常状态所需的全部材料，零备件，劳务及差旅费用。

电话支持　　一周 7 天，每天 24 小时

本项目的用户在使用 Sun 公司产品时如遇到问题， 无论是软件或硬件， 都可以从 Sun 公司得到电话支持与帮助。 用户可以指定一名主要联系人及两名替补联系人与 Sun 公司客户服务部联系。一旦接到用户请求电话， Sun 客户服务部的专家将在规定时间内通过电话解决或回答用户所提出的问题。

现场支持　　周一至周五，9：00 至 18：00 （节假日除外）

对于通过电话无法解决的硬件系统故障，Sun 公司将派出系统工程师到用户现场为用户解决问题。

硬件系统响应时间的定义

铁道部项目各级用户定义优先权	电话响应	现场响应
紧急(系统瘫痪)	立刻响应	4 小时内(本地)
严重(系统严重故障)	2 小时内回复	一个工作日内(本地)
一般(系统一般故障)	4 小时内回复	尽早响应

注：“ 本地 ”指距 Sun 公司办事处或支持中心 50 公里以内的地区，Sun 公司目前分别在北京，上海，广州和成都设有办事处，在沈阳，天津，济南，西安，杭州，长沙，无锡，南京，武汉，合肥，福州，深圳，南宁，贵阳，昆明及重庆设有支持中心。对其它地区的现场响应时间将根据交通状况确定

并尽快解决，一般在 1 — 2 天。

Sun ONE 软件响应时间的定义

铁道部项目各级用户定义优先权	电话响应
紧急(系统瘫痪)	1 小时内回复
严重(系统严重故障)	2 小时内回复
一般(系统一般故障)	4 小时内回复

远程分析 (Remote Dial-in Analysis)

必要时，本项目各级用户可以采用 Sun 公司的远程分析服务。通过适当的信关(Gateway)，Sun 公 司客户支持中心的专家对本项目的系统进行远程诊断， 加速问题的解决。

替换硬件零部件

Sun 公司分别在北京，上海，成都和广州设有零备件中心，为本项目各级用户就近方便快速地更换零部件。替换的零部件通常已按 Sun 公司的更换规则进行了必要的升级，以优化本项目各级用户的系统性能。

版本升级与增强

Sun 公司的增强版本可能包括新的功能和特征， 对已发现问题的修正及对新硬件平台的支持。 本项目的各级用户会收到最新的 Solaris 软件，还可以得到最新的有关 Solaris 和任何经 Sun 公司发放许可的非随机软件(Unbundled)的修补软件(Patches) 维护版本(Maintenance Release).

Sun ONE 软件产品的三年内版本升级费用将含盖在 Sun ONE 软件产品三年的维护支持服务中. 用户可以根据 Sun 公司提供的指定站点下载软件升级版本及补丁程序.

SunSolve 许可证

SunSolve 是一个综合性维护数据库，其中包括最新的系统支持手段及各级用户经常提出的问题及解答，软件缺陷（Bugs）的描述和修补程序 (Patches)，技术注释及其它对各级用户解决技术问题有帮助的信息。在线(Online) 版本每天更新，本项目各级用户可以通过 Internet 实时读取有关信息。

EarlyNotifier (提前通知)服务

Sun 公司通过 EarlyNotifier (提前通知)服务将公司刚刚发现的重要问题与 Bugs 及时通知各级用户，使其防泛于未然。

多厂商支持计划：(VIP)

Sun 公司与业界主要的软件厂商建立了紧密的支持联盟合作关系，解决了 Sun 公司产品与这些厂商的软件的支持相互支持的可操作性的问题，为拥有 Sun 公司关键业务服务的客户并同时具有同等级别的联盟软件厂商的软件支持服务合约的客户提供一站式的服务窗口，避免了在服务中故障定位不清，客户穿梭于硬件和软件厂商的情况，彻底提升服务响应和故障解决的质量。

SUN 公司特别提供 Web-Based 在线支持中心（OSC）

（OSC）在开始向 IT 客户提供服务之初，便处于客户服务的最前沿。OSC 在亚太地区是第一个提供企业级支持服务的电子商务。简而言之，Sun 的 OSC 是全新的覆盖全球的客户 Web 接口，客户只需轻敲键盘就能在线获得服务，它改进了 Sun 企业级服务与客户的交互方式。

OSC 在最前沿提供有效的企业级服务，它与每个客户建立了直接的、个性化的增值联系，因而在 IT 系统服务领域处于领先位置。同时，通过将服务自动化以及在线解决与服务相关的问题，OSC 使得 Sun 企业级服务能够更有效地利用我们的资源。

提供 OSC 的目的，是为了通过更有效地在线交互式共享数据和信息，提高客户的满意度和客户响应速度，使得 Sun 企业级服务模式对客户而言更接近于自助管理。

OSC 将为在线服务的传递提供重要的功能。现有的功能包括，客户提交服务请求（SR)、监视状态、跟踪 SR 的进展、以及在线查阅合同信息的功能。

对铁道部用户而言。OSC 的一大优点是，可以以更快的速度、全天候得到故障排除和自我管理。在用户提交服务请求之前，OSC 提示用户搜索知识库以尽可能解决客户的问题，为客户避免不必要的花消。

9.5.4 9.5.4 客户问题报告程序

为保证铁道部项目的客户的故障报告得到优先响应，特明确问题报告程序如下：

1．各级用户指定专门的系统管理员或联系人。在使用 Sun 产品过程中发现问题

时，请首先反映给指定联系人，由联系人与 Sun 客户服务部联络。

2．指定联系人在向 Sun 客户服务部报告技术问题时，请描述清楚问题的症状，包括给出详细准确的出错信息，错误代码等，便 Sun 客户服务部能更好地优先响应和解决您的问题。

在保修期中，如果系统在运行过程中出现紧急情况，请立即拨打 Sun 公司 800 号热线电话请求帮助：

1. 拨打 800-810-0035；
2. 告知服务合同号（此号码会在设备安装后提供）与设备序列号；
3. 详细说明故障现象；
4. 配合工程师做进一步检测；
5. 如需现场支持，请保护好现场并做好相应安全措施，等待工程师做现场服务。

9.5.5 服务追踪及客户故障记录

所有本项目的故障记录将保持 SUN 公司客户服务数据库中，客户可通过 WEB 进行查询，并追踪问题解决状态。

9.6 客户支持中心信息

Sun 公司技术支持中心（Solution Center）：负责整个中国地区的电话支持服务

服务热线： 800 – 810 0035 （7x24 小时免费电话）
010 - 68042508
寻呼热线： 010 - 96300 呼 311393
传真： 010 - 68020220
E-mail： ask@prc.sun.com

9.7 SUN 公司服务体系介绍

9.7.1 Sun 客户服务部介绍

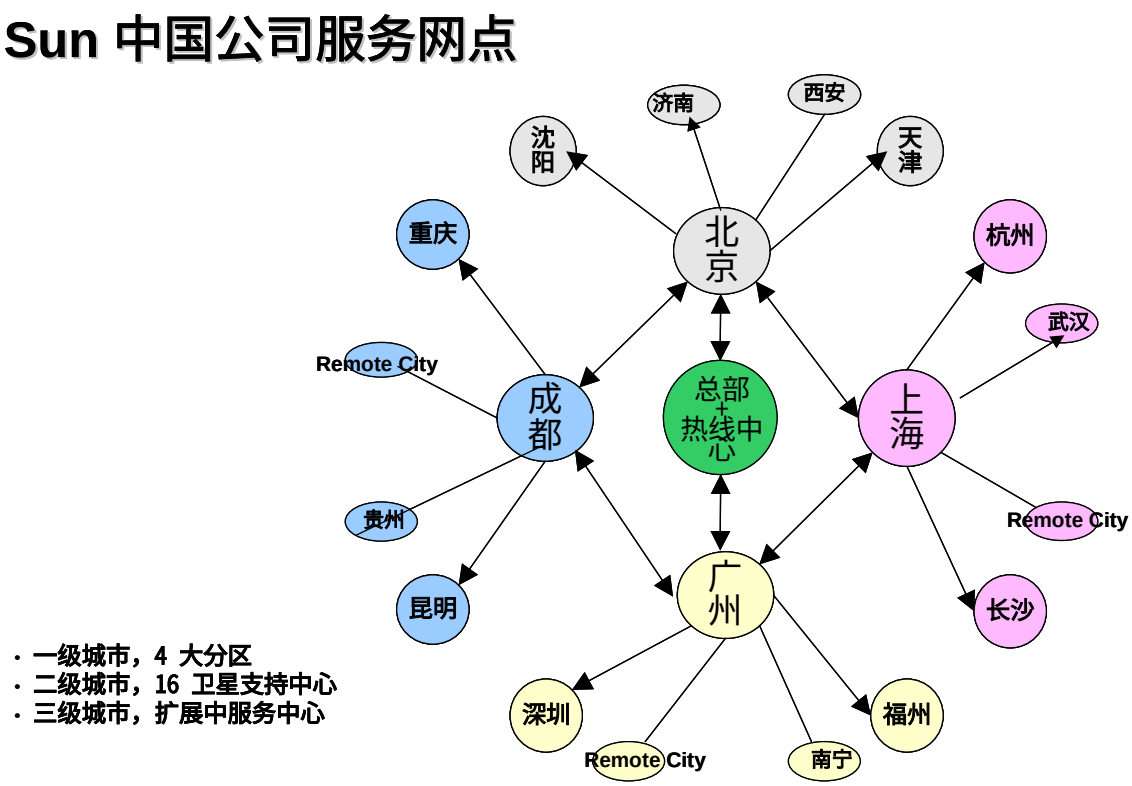
Sun 公司不仅以其高技术、高质量、高可靠性的计算机、 存储设备，以及先进

的 UNIX、JAVA 技术而著称于业界；同时，其技术支持和售后服务也以其灵活、高效、全面（系统支持 维护、培训、IT 顾问咨询和系统集成等服务）和高质量成为全球 UNIX 系统支持、服务及培训的第一名，普遍得到广大用户的赞誉。

Sun 客户服务部是 Sun 公司专门提供售后支持服务和培训的部门，Sun 客户服务部的技术人员将会负责硬件，操作系统安装、调试工作，并将负责整个系统的售后技术支持维护，保修及后期的维修服务。

9.7.2 中国客户支持中心

自九十年代初以来，为了更好的为中国用户提供服务，Sun 公司在中国建立了完善的一体化服务体系， 分别在北 京 、上 海 、 广 州、成 都、深 圳、 天 津、沈 阳、济南、西安、长 沙、杭 州、南京、无锡、武汉、合肥、南宁、贵阳、重 庆、福 州 和 昆 明设立技术支持和售后服务中心， 同时在北 京 、 上 海、广 州 和成 都 设立零备件保税仓库。Sun 客 户服务部中国区共有 100 多名专业技术支持员工来提供对整个中国地区的售后支持服务。目前，直接和 Sun 客户服务部签订技术支持和服务的客户有 500 多个， 遍布全国 31 个省市 、 自治区， 所支持的系统从高档服务器 、 存储设备到工作站共约 5000 多台套 。



Sun 公司全国客户支持中心的具体分布和人员情况如下表：

区域	地址	电话	人数
北方区（北京）	北京市南礼士路 66 号，建威大厦 16 层。邮编：100045	010-68035588	37 人
华东区（上海）	上海市淮海中路 1325 号百富勤大厦 18 层。邮编：210031	021-64661228	35 人
华南区（广州）	广州市天河北路 138 号，大都会广场 4004-4015 室。邮编：510620	020-87555900	32 人
华西区（成都）	成都市人民南路二段 18 号，川信大厦 11 层 C 座，邮编：610016	028-86199333	23 人
电话技术支持中心（北京）	北京市南礼士路 66 号，建威大厦 16 层。邮编：100045	800-810-0035	10 人

9.7.3 备件库

SUN 公司在如下 4 个城市设有零备件保税仓库：

- 北京
- 上海
- 广州
- 成都

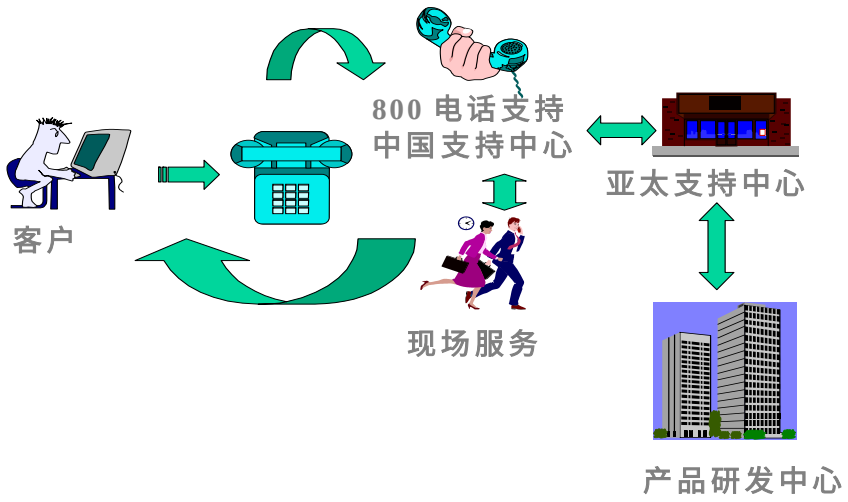
在各地服务中心也相应存有零部件，以加快用户的故障解决速度。

9.7.4 新系统的支持和培训

Sun 公司为用户提供高质量的全生命周期内的系统支持服务， 每当新系统正式交货发布时，SUN 公司对所有支持服务的工程师提供预先的测试安装系统化培训，保证所有支持工程师都获得专业化的技术认证。同时，所有的备件库也将存放的新系统的备件，以保证用户在采用 SUN 公司最新技术的同时，能够得到 SUN 公司全面，专业，及时，快速的服务。

9.7.5 Sun 客户服务部技术支持模式

针对此招标项目工程实施的具体情况， SUN 客户服务部提供以下三级支持模式：



- **本地支持(第 一 级)**

Sun 客户服务部在各地服务中心系统工程师为本项目的用户提供包括对硬件、软件、网络应用和网络相互操作性问题等的一体化的电话和现场支持服务，我们同时提供 800 号免费热线服务电话、远程拨入分析、SunSolve CD 数据库分析等， 这一切都保证铁道部用户的系统能够正常运转。对本项目中 Sun 公司设备及软件出现的问题我们承诺电话响应优先回答，并根据需要提供及时的现场服务以解决疑难问题，如果本地的技术咨询中心不能很快有解决方案，我们会及时把您的问题升级到设在新加坡亚太升级中心 (AEC – Asia Escalation Center)。

- **AEC 亚太升级中心（第二级）**

位于新加坡的亚太升级中心是为亚太地区各个国家的 Sun 的技术咨询中心提供后备支 援的机构。亚太升级中心采用 Sun 公 司最先进的工具和技术手段使用户的技术问题尽快 得到解决。如果本项目的用户的问题 (bug) 在 AEC 不能马上解决，AEC 亚太升级中心会把您的问题反应到 Sun 公司总部的产品开发研究中心 (P&D

- Product & Development)。

- **CTE (Corporate Technical Engineering) 产品研发中心 （第三级）**

设在美国硅谷的 Sun 公司产品开发研究支持中心,其作用是使 Sun 公司在全球的用 户的一些共同的疑难问题得以解决，并且尽快为您提供问题的解决方案。

9.7.6 ISO9002 的服务体系品质管理认证

SUN 公司的服务体系管理，服务质量保证体系已获得 ISO9002 国际标准认证。

9.8 本项目技术支持与服务的主要人员

Sun 公司负责本项目技术支持和服务的主要人员和职责如下表：

编号	人员姓名	职 务	联系电话	主要职责
1	刘建坤	客户服务区域总经理	68035588-28889	项目服务监督
2	王威	服务客户经理	68035588-82648	项目服务计划制订及优化
3	刘开京	技术服务经理	68035588-28902	项目服务技术支持管理
4	黄海	服务技术支持中心经理	68035588-28782	项目服务质量监督

项目实施领导小组：

刘建坤， 王威，刘开京， 温国彬, 李晓琪

项目实施小组：
SUN 总部及全国各分公司的售后服务工程师。

北方区 ：北京市南礼士路 66 号，建威大厦 16 层。（100045） 电话：010－68035588
区域负责人：刘建坤 电话：010－68035588 ext.28889

实施工程师：

分机号	人员姓名	职务	工作年限	参加实施的主要工程项目
28903	孟祥波	客户技术经理	13 年	安钢公司信息网与 IBM SNA 网的接入安装及配置；韩国三里公司数据库系统及工厂物管系统建立与支持；北京华侨饭店管理系统支持与维护；邮电部长话局计费系统；电信管理局信息系统；山东移动局计费系统；上海证券交易所；北京证券交易所交易系统；深圳平安保险公司寿险业务；上海自行车三厂数据库系统；成飞公司/沈飞公司 MRP 项目；参与创建中国惠普响应中心、电话服务中心；实施高可靠性支持服务；中国爱立信公司信息技术部电子邮件服务器及 DNS 安装、维护；北方电讯公司工厂管理系统实施及安装；DHO 建行业务系统集群服务器安装、维护；南京金黄色陵石化 X.25 网络系统建立、配置、维护；外经贸部 EDI 协议的配置、维护；国家气象局 HDLC 协议的卫星网的接入配置；原计划生育委员会信息管理系统安装、咨询 为在中国区初稿“白金服务计划”及主动式服务方式组织、培训技术队伍，制订具体实施方案；规划、完成所有问题项目；天津摩托罗拉数据库项目管理、负责管理重要客户服务的实施
28915	姚　琦	系统支持工程师	22 年	黑龙江省中行、东方数据处理公司 E10K 设备的安装调试；重庆 169 工程项目 HA Cluster 的安装调试；河北沧州移动局 PDB Cluster 系统环境维护；多次为客户安装调试 E3X00、E4X00、E5X00、6X00 系列服务器及 A5000 磁盘阵列；
28777	郭　键	系统支持工程师	7 年	参加了海总指挥系统开发工作；装甲部队辅助系统开发 铁道部票务计算机管理项目的系统安装调试；贵州省移动计费系统的安装调试

28901	冯晓露	系统支持工程师	8 年	CAAC Cluster 安装、维护；中行宁夏分行 Cluster 的安装、维护；北京市电话局 97 工程主机系统安装、维护
28519	潘军	技术支持经理	12 年	深圳招行 E10K 安装 南海中行 E10K 安装 福建移动 Sun PDB 安装 广东移动计费系统维护

华西区：成都市人民南路二段 18 号，川信大厦 11 层 C 座。（610016）电话：028－86199332
区域负责人： 王志涛 电话：028－86199333 ext.84221
实施工程师：

分机号	人员姓名	职务	工作年限	参加实施的主要工程项目
84229	许 进	服务支持工程师	7 年	高级技术支持工程师，参加过的主要项目有贵州移动 BOSS 项目 SF6800 CLUSTER 系统的安装维护支持，西藏移动 BO SS 项目 SF3800 CLUSTER 系统的安装调试。
84234	戴芒芒	服务支持工程师	7 年	高级技术支持工程师，主要参加的项目有四川移动 BOSS 项目 SF6800、E10000 CLUSTER 系统的安装调试，现任该项目主管工程师。
84242	谢庆涛	服务支持工程师	10 年	高级技术支持工程师,参加重庆移动 BOSS 项目 SF15K 三节点 CLUSTER 系统的安装调试。

华东区：上海市淮海中路 1325 号百富勤大厦 18 层。（210031）电话：021－64661228
区域负责人： 徐建平 电话：021－64661228 ext.41080
实施工程师：

分机号	人员姓名	职务	工作年限	参加实施的主要工程项目
41079	宓闪珂	技术服务经理	15 年	资深技术专家，15 年 IT 领域技术经验，近 11 年的大型系统实施经验。在 SUN 公司成功领导实施了宝钢信息中心，上海热线 email 系统，上海银

				行，**BeIII 研发中心，上海 163，南昌商业银行，湖南网管，湖南移动 2000，华为，中石化 ERP，中芯国际，安徽移动 BOSS 系统，太平洋保险等数十个系统集成项目，**现任 SUN 华东区技术服务经理.
41077	吴龙富	服务支持工程师	12 年	高级技术支持工程师，主要参加 Seagate 公司生产管理系统 5 套 SF6800 系统的安装、实施及技术支持；江苏移动网管系统，浙江国税征收系统，AMD 苏州生产管理系统的安装维护；上海环球网络 CLUSTER 系统，苏州旭电，浙江联通 CLUSTER 系统，爱立信上海研发中心技术支持。
41091	何建军	服务支持工程师	7 年	高级技术支持工程师，参加江苏 163Email 系统的安装调试，中国工商银行上海分行网关系统的安装、维护，中芯国际 F15K 的安装调试，参加安徽移动计费业务系统 F15K、F6800 项目的安装调试。
41082	徐玮	服务支持工程师	8 年	高级技术支持工程师，参加南昌市商业银行、上海银行、中国工商银行上海分行 E10K 系统安装、调试及技术支持；UTStarcom 小灵通业务的系统安装、调试和实施。
41025	潘怡鸿	服务支持工程师	6 年	高级技术支持工程师，参加湖南网管，湖南移动 2000，上海热线 SRS 的实施与维护，上海电信 IP 旁路，德国 GedasE10K，安徽移动 BOSS 系统,安徽烟草 SF6800，安徽 ICBC 系统安装、调试和维护。

华南区：广州市天河北路 138 号大都会广场 4004-4015 室。（510620） 电话：020－87555900
区域负责人： 张传峰 020－87555900 ext.58848
实施工程师：

分机号	人员姓名	职务	工作年限	参加实施的主要工程项目
58843	尹德晓	技术服务经理	17 年	资深技术专家, 17 年 IT 领域技术经验, 近 9 年的大型系统实施经验。**在 SUN 公司成功领导实施了福建移动计费，广东电信 97 工程，华为 IT 数据中心，广东移动计费，OA 及网管，平安人寿保险数据中心等数十个系统集成项目，**现任 SUN 华南区技术服务经理.
58870	郑强	服务支持工程师	8 年	高级技术支持工程师, 主要参加中国工商银行广东分行，广东省公安厅，青海证券、湛江西部石油的 E10K 系统的安装、实施及技术支持；海南移动计费系统、易方达基金管理公司的 SF4800 系统安装、调试及技术支持。
58845	吴勉熙	服务支持工程师	9 年	高级技术支持工程师,参加福建泉州电信计费 E10K 系统安装、调试及技术支持；福建电信 163 计费 SF4800 系统的安装、调试和实施;福建移动 4 节点 cluster 技术支持。
58865	张劲松	服务支持工程师	8 年	高级技术支持工程师, 参加中国工商银行广东分行 E10K 系统安装、调试及技术支持；广东电信计费系统 Sunfire 4800 项目安装、调试；湛江西部石油的 Sunfire 4800 系统的安装、实施及技术支持;广东美的空调 Sunfire4800 系统的安装、实施； 广州软件园 Sunfire4800 系统安装，调试，技术支持。

9.9 PS 咨询服务的支持

1. 项目实施阶段的紧急响应流程：

项目实施阶段，PS 的咨询服务人员在现场进行项目的实施。因此，如果关于 PS 咨询服务部分的紧急问题发生，PS 专业咨询服务人员将在现场进行立即响应，帮助分析和解决问题。PS 专业咨询服务人员的第一联系人为 PS 项目经理，第二联系人为 PS 技术总负责人。

项目经理暂定为：吕艳平，联系电话：13801170856

2. 免费维护期内 PS 的紧急响应流程：

用户验收后，进入三个月的免费维护期。三个月的免费维护期内，如果关于 PS 咨询服务部分的紧急问题发生，PS 会指定专人专职负责在双方合同规定的时间内进行快速响应，帮助客户分析和解决问题。具体的联系人将在项目移交给客户之前确定，此人会具有相应的技能和经验。

3. MA 期间 PS 的紧急响应流程：

三个月的免费维护期过后，进入维护期间（MA）。需要客户购买维护服务。如果客户购买了维护服务，在维护期间内，关于 PS 咨询服务部分的紧急问题发生，PS 会指定专人专职负责在双方合同规定的时间内进行快速响应，帮助客户分析和解决问题。具体联系人将在 MA 合同商讨时确定，此人会具有相应的技能和经验。