



国家电子政务外网 电子认证服务体系白皮书

国家电子政务外网数字证书中心

目 录

1	概述.....	1
1.1	政务 CA 的使命	2
1.2	政务 CA 的服务宗旨	2
1.3	政务 CA 的愿景	2
1.4	管理与服务机构	3
2	全国认证服务体系建设.....	5
2.1	电子认证服务体系建设情况	5
2.2	基础设施建设情况	6
3	电子认证服务开展情况.....	错误!未定义书签。
3.1	业务开展情况	错误!未定义书签。
3.2	证书服务和管理	错误!未定义书签。
3.3	合规及运维情况	错误!未定义书签。
3.4	服务能力与优势	错误!未定义书签。
3.5	应用案例	错误!未定义书签。
4	服务内容.....	6
4.1	证书服务	13
4.2	密码服务	13
4.3	业务网络接入	13
4.4	安全身份认证网关	14
4.5	单点登录服务系统	15
4.6	签名验证服务系统	17
4.7	电子签章系统	19
4.8	时间戳服务系统	19
4.9	本地用户注册系统	21

1 概述

国家电子政务外网数字证书中心(政务 CA)是经国家密码管理局核准并授予电子政务电子认证服务资质,由国家电子政务外网管理中心电子认证办公室管理的面向各级政务部门及其所属单位,以数字证书方式为主,提供数字认证、授权管理和责任认定等网络信任体系领域的专业化服务机构。政务 CA 运营的电子认证服务体系,是目前国内唯一可以为党委、人大、政府、政协、法院和检察院的各级部门纵向业务和各部门之间的横向业务提供电子认证的服务体系,承担了为中央政务部门延伸到各地方的业务应用系统提供电子认证服务的任务。该体系采用全国“一证通”机制,保障了跨部门、跨地区数据安全交换、信息资源共享和业务应用协同的安全联通,解决了目前电子政务领域“条”和“块”之间认证信息不统一的问题。

政务 CA 电子认证服务机构采用在国家-省-市三级分级部署方式,能够为各级政务部门用户提供全国统一标准的身份认证、授权管理、责任认定、密码管理等电子认证服务,是各级政务部门可以信赖的提供网络信任服务的“国家队”。通过提供对人员、机构、设备、数据和应用等资源的可信管理服务,为各级政务部门的电子政务、公共服务、信息惠民工程、智慧城市建设营造安全的应用环境,实现信息安全共享、业务安全协同和网络安全互联,为建设网络强国、步入信息社会和实现中国梦、做出应有

的贡献。

1.1 政务 CA 的使命

一是保障政务外网网络安全。为接入、部署和运行在政务外网上的设备、人员和业务应用提供身份认证、授权管理和责任认定服务。

二是保障政务业务安全。为使用电子政务应用的各级政务部门的公务人员、授权机构提供身份认证、授权管理、责任认定服务，为政务业务软件和业务应用提供代码签名服务。

1.2 政务 CA 的服务宗旨

满足各级政务部门跨部门、跨区域的业务要求，政务业务应用延伸到哪里，政务 CA 就服务到哪里。

按照“统一规划、统一标准、统一服务”的要求，提供中央、省、市的三级网络信任服务。

以“政务 CA”为统一品牌，依托各地电子认证注册服务中心，实现统一标准的属地化管理及服务，实现全国“一证通”服务。

1.3 政务 CA 的愿景

成为国家级的电子政务网络信任基础设施，成为各级政务部门信赖的、权威的网络信任服务机构，面向政务网络空间提供自主可控的网络信任服务。

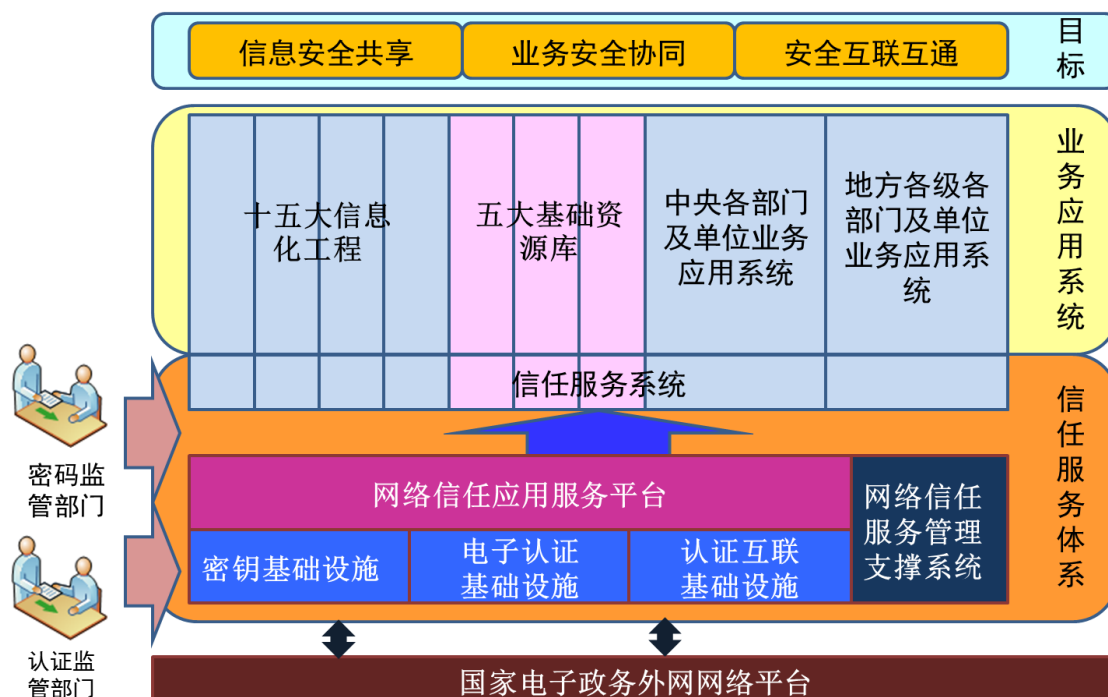


图 1. 在国家电子政务领域的定位

1.4 管理与服务机构

2010 年国家发展改革委人事司批准成立“国家电子政务外网管理中心电子认证办公室”，主要职责是负责电子政务外网数字证书认证业务的相关管理、运行和服务工作，是国家电子政务外网电子认证工作统一对外管理和窗口；电子政务外网电子认证服务工作由国家电子政务外网数字证书中心承担。

2010 年 6 月 4 日，国家密码管理局发文同意国家电子政务外网数字证书中心开展电子政务电子认证服务。2011 年 3 月 30 日，国家密码管理局为国家电子政务外网数字证书中心颁发“电子政务电子认证服务机构”服务资质牌匾。



图 2. 电子政务电子认证服务机构资质

1.5 政策文件要求

按照中央有关文件精神 and 《关于加强和完善国家电子政务工程建设管理的意见》（发改高技〔2013〕266 号）文件要求，统一使用国家网络信任服务设施；部署在国家电子政务外网上的业务应用要统一使用电子政务外网平台提供的信任服务设施；已建和新建的电子政务项目，有关部门要同步使用国家电子政务内网和国家电子政务外网平台提供的信任服务设施。

另外，《关于进一步加强政务部门信息共享建设管理的指导意见》（发改高技[2013]733 号）文件还要求，依托国家电子政务网络信任设施，利用有关部门和地方已建电子认证系统，为政务信息共享提供身份认证、授权管理和责任认定等安全服务。

2 全国认证服务体系建设

2.1 电子认证服务体系组织结构

政务外网电子认证服务体系的组织结构采用树状。其中，国家政务外网数字证书中心配置 CA 系统，承担政务外网电子认证管理和具体服务工作；省注册服务中心是经国家电子政务外网管理中心电子认证办公室批准，为省级和以下政务部门提供电子认证服务和管理的省级机构，配置 RA 系统；市注册服务分中心是经省注册服务中心批准、为市级以下政务部门提供电子认证服务的市级机构，配置 LRA 系统；注册服务点是经省注册服务中心批准，为当地政务部门或特定业务对象提供数字证书服务的受理点，配置 LRA 系统。

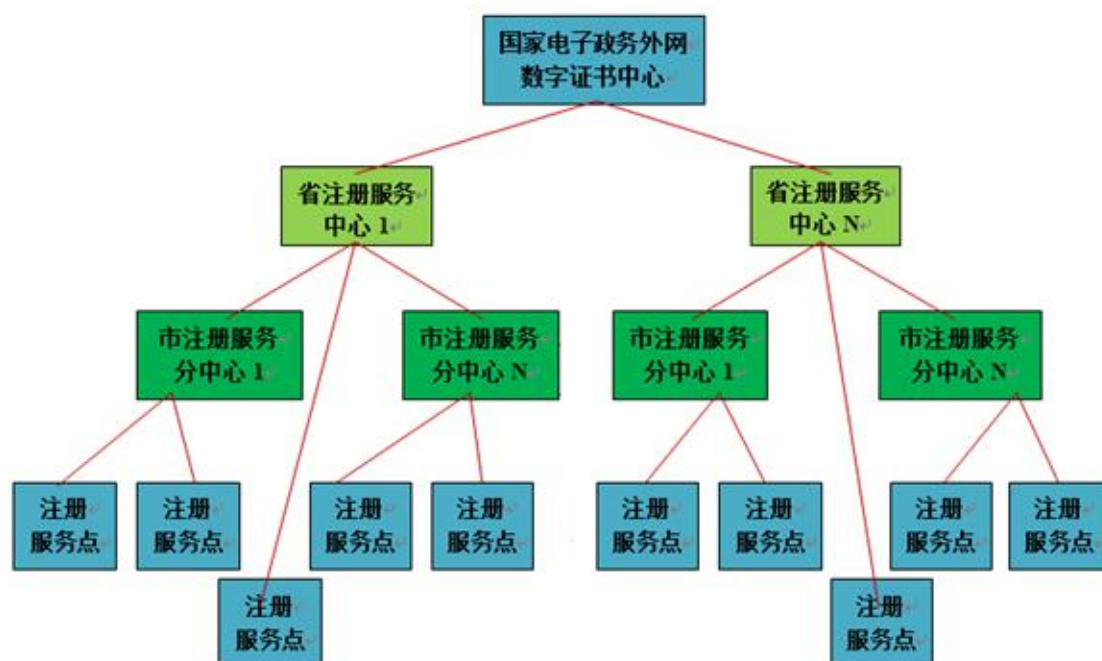


图 3. 国家电子政务外网电子认证服务体系布局结构

到 2013 年底，政务 CA 建设完成 22 家省级电子认证注册服

务机构，7 个中央部委建设了为本级部委服务的 RA 系统，初步形成全国电子认证服务体系框架。

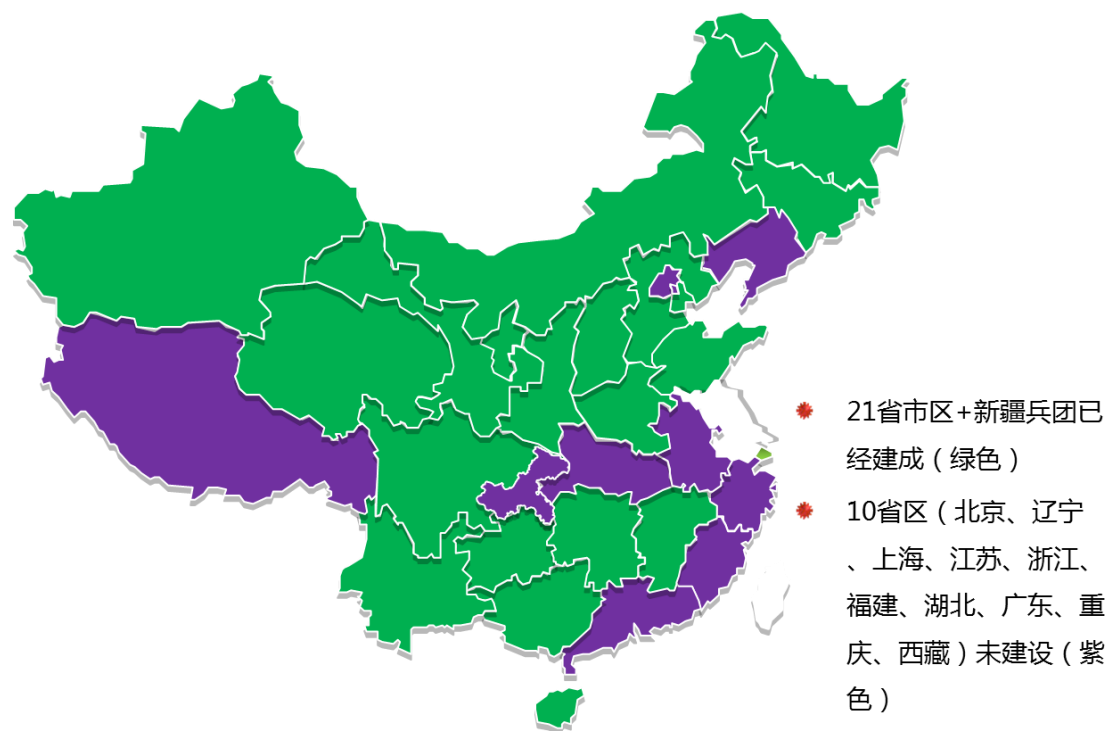


图 4. 全国电子认证注册服务机构分布情况图

2.2 基础设施建设情况

按照国家密码管理局的要求，政务 CA 建设了国家政务外网密钥管理基础设施，为政务外网上运行的业务系统提供商用密码服务。

2.3 业务开展情况

政务 CA 为接入国家电子政务外网的政务部门、应用系统和用户提供集中统一、安全可靠电子认证服务，保障电子政务活动的正常有序开展。至 2013 年底，国家电子政务外网数字证书中心已经为国家发展改革委、国土资源部、监察部等 21 个部委、230 多个电子政务应用提供了身份认证、电子签名、数据加密、时间戳等网络信任服务；为山东省、安徽省、四川省等 15 个省市、68 个电子政务应用提供了身份认证、电子签名、数据加密、时间戳等网络信任服务，共发放 20 余万张数字证书。

主要应用情况如下：

注册机构	应用单位	应用系统
国家 RA	中华全国总工会	全国工会系统网络工作平台
	国务院扶贫办	全国扶贫数据上报系统
	中国民主建国会	民主建国会电子会务平台
	国家信息中心	外网网站维护、 信息处全国上报数据
	国务院纠风办	中纪委纠风系统
	农业部	部内业务
	监察部预防腐败局	国家预防腐败局网站维护
	国务院应急办	全国应急系统
	新华通讯社	远程管理托管在国家信息中心机房 内的服务器
	最高检察院	案件信息公开系统
	中央国家机关 人民防空办公室	人防管理系统
	发改委	12358 价格监督举报系统
	国家安全生产监督 管理总局	安监应用系统
审计署 RA	审计署	审计署内应用 20 多，18 个特派办全

		部大概 200 个左右应用
环境保护部 RA	环境保护部	环境保护部内业务系统
国家发改委 RA	国家发改委	用于委内 7 个业务系统
民政部 RA	民政部	民政部内业务系统
国土资源部 RA	国土资源部	国土资源部内业务系统
国家质检总局 RA	国家质检总局	国家质检总局内业务系统
国家地理资源 RA	国家地理资源局	国家地理资源局内业务系统
安徽省 RA	安徽省发改委、财政厅、阜阳市政府、六安市等	安徽省财政采购平台，省发改委，阜阳市政府、六安市政府办公系统等
山东省 RA	山东省发改委、山东省卫生厅等	山东省发改委内业务、山东省卫生厅医药采购平台等
四川省 RA	四川省宜宾市	四川省宜宾网上办公平台
云南省 RA	云南省政府、保山市	门户网站后台发布系统、保山市协同办公系统
贵州省 RA	贵州省卫生厅、遵义市	贵州省卫生厅医药采购平台、遵义市政府网上办公系统
海南省 RA	中共海南省委、省政府、三亚市政府	省领导信息系统、省委省政府 OA 系统、省公务员门户、12380 举报网站项目系统、省卫生厅、省农业厅、海南省文体厅、食品药品监督管理局 OA 系统；三亚市人民政府行政审批系统、卫生局、党政 OA 系统等

2.4 证书服务和管理

政务 CA 提供的证书服务包括：

- 机构和个人用户的身份审核、资料管理等；
- 证书生命周期管理，如证书签发、更新、冻结、注销、在线查询等；
- 客户服务，如 PIN 码设置、解锁、终端安装指导等；
- 相关应用技术支持，如网关接口、黑名单设置、部署方

案等。

政务 CA 认证服务体系依据属地化服务原则，由各级注册服务机构为本地用户签发数字证书，并进行客户服务、在证书生命周期内满足用户的各项需求。整个认证服务体系按照统一的服务标准规范（由国家电子政务外网电子认证办公室制定）进行各种操作和服务。

用户依据证书申请流程中的要求准备申请材料和表格，准备齐全后提交到本地注册服务机构，由各级注册服务机构审核无误后，签发数字证书给用户。

2.5 合规及运维情况

目前全国认证服务体系运行和维护由政务 CA 和地方省注册服务中心共同负责。

运维人员均按照《国家电子政务外网 CA 认证系统人员管理制度》进行管理，并签署保密协议。

在系统安全管理方面，制定了多项规章制度，包括《国家电子政务外网 CA 认证系统安全管理办法》、《国家电子政务外网 CA 系统应急响应计划》、《CA 认证系统备份和恢复方案》等

运维服务人员提供 7×24 小时状态监控、故障处理，5×8 小时客户服务、技术支持等服务，保障系统的安全平稳运行。

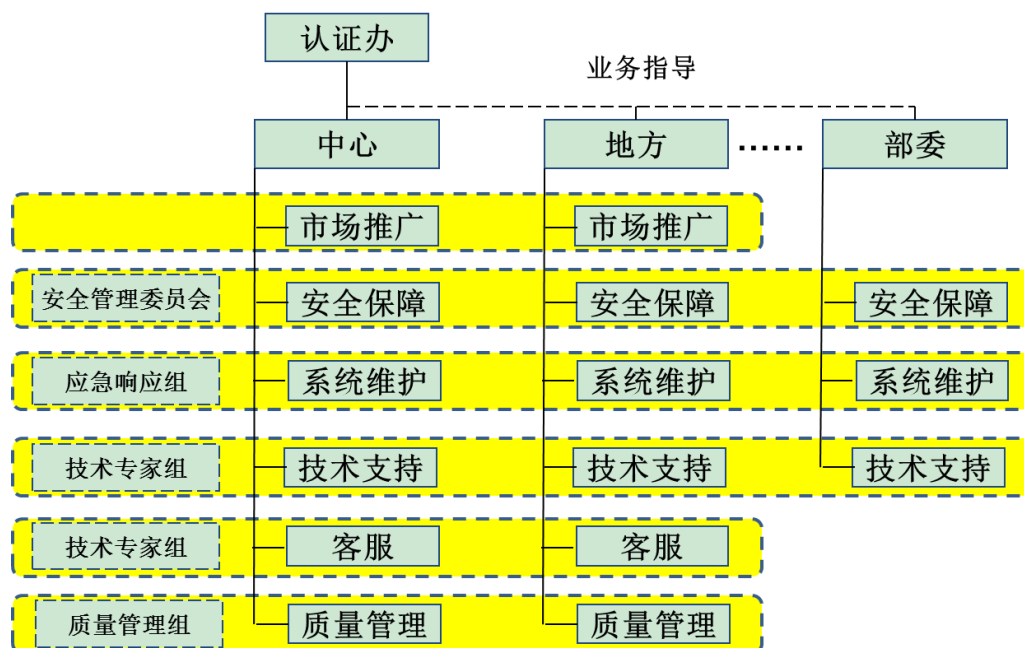


图 5. 全国认证体系的运维与服务架构图

同时，制定了《国家电子政务外网 CA 认证系统安全管理办法》，建立了由部门主管主任为领导的安全管理委员会，由认证服务处等相关部门组成的安全管理机构。

制定了《国家电子政务外网 CA 系统应急响应计划》和《CA 认证系统备份和恢复方案》。

2.6 服务能力与优势

发布了《国家电子政务外网认证业务规则》，同时制定了证书生命周期管理的《证书管理规范》系列以及包含客户服务管理、服务人员配置、质量管理、工作制度、客服工作指南、客服准则、证书使用指南、培训、满意度调查等方面系列《服务管理规范》。

具有多层次的技术服务支撑体系，包括：互联网服务网站，提供热线电话、在线 QQ、信箱服务手段，技术专家支持等。

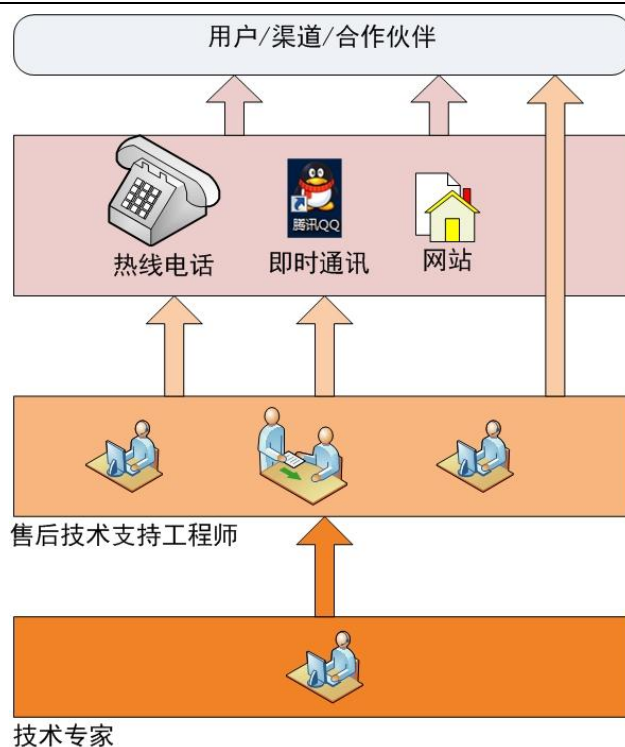


图 6. 服务支持体系图

在线自服务系统：用户可通过自助在线更新系统延期证书有效期。



图 7. 在线证书更新系统

管理平台：



图 8. 政务 CA 综合管理平台

门户网站: www.stateca.gov.cn



图 9. 政务 CA 门户网站

● 全国一证通

采用的数字证书的技术标准一致、格式统一，网络信任服务体系在全国范围内提供统一的数字证书服务，实现政务外网范围内数字证书“一证通”。国家部委从中央到地方的全国性业务，只需和认证中心进行单点业务接洽，即可获得全国范围内的认证服务与技术支持。使跨部门、跨地区信息资源共享、业务协同、

数据安全交换，及业务应用的安全互联互通成为可能。

● 属地化服务

属地化服务分为两个层面：认证服务中心（中央）层面和注册服务中心（省级）层面。认证服务中心负责给中央国家机关提供正式服务；注册服务中心为本省内的证书应用提供服务。充分利用政务外网在全国的资源以及其完备的服务体系，在当地提供包括证书申请、发放、修改、更新、挂失等服务，就近满足用户的需求，其属地化服务的特点使服务方式更便捷、更高效。

3 服务内容

3.1 证书服务

通过电子认证基础设施为电子政务业务系统提供签发、注销、更新等基础证书服务；能够提供机构证书、个人证书、设备证书和代码签名证书等服务。

3.2 密码服务

第三方电子认证基础设施能够为电子政务业务系统提供不同种类密码服务，包括对称密码管理服务，非对称密码管理服务，密码应用合规性检查和密码应用有效性检查服务。

3.3 业务网络接入

对于业务应用系统部署在国家电子政务外网或者用户单位的内部业务网络的情况，可以在互联网和业务网络的边界部署

VPN 网关，用户使用数字证书通过 VPN 网关从互联网访问内部业务系统，用户终端和 VPN 网关之间实现安全加密传输，数字证书实现了接入用户身份的强身份认证。

3.4 身份认证网关

身份认证网关是专用安全产品，为应用系统提供基于数字证书的高强度身份认证、高强度数据链路加密等安全服务，保障应用系统用户登录安全。

身份认证网关部署在应用客户端（包括浏览器）与应用服务器（包括 Web 服务器）之间，使用数字证书完成双方的身份认证，在服务器端和用户客户端建立高强度的 SSL VPN 加密连接，实现客户端和服务端之间身份的有效认证和数据传输安全。身份认证网关使用代理（Proxy）应用模式，即身份认证网关对所有经过的网络流量都进行处理，然后传递给被保护的服务器，因此用户必须通过身份认证网关才能访问被保护的服务器。

身份认证网关可以部署为串联模式（桥模式）或者并联模式（单臂模式）。推荐使用并联模式，并联模式下安全身份认证网关不使用内网口，而使用外网口直接接入业务应用系统所在的网段交换机。从用户使用逻辑上，其仍相当于在用户和被保护的应用服务器之间，对用户信息进行认证保护，当认证不通过时，禁止其访问相关应用。

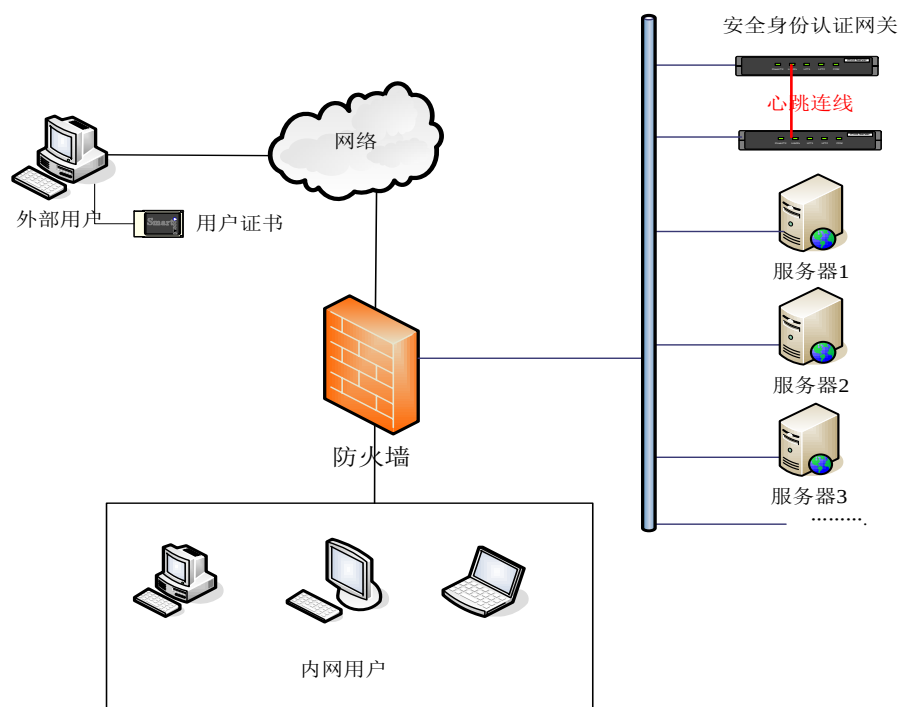


图 10. 安全身份认证网关部署示意图

系统支持双机热备功能，在需要高可靠性的环境下需要对网关进行双机热备部署。双机热备部署需要部署两台设备，一台作为主机，一台作为备机，两台机器都与网络连接，两台设备之间使用交叉线连接热备口进行状态检测，在正常情况下由主机提供服务，当主机发生异常时系统自动切换到备机进行服务。

3.5 单点登录服务系统

单点登录功能通过整合现有的应用系统登录入口，实现多应用间的安全单点登录。实现基于数字证书的用户只需一次登录，即可在多个信息系统中自由、安全切换。通过边界接入安全网关实现与应用系统（B/S 或 C/S 架构）进行的无缝接入，达到最小化改动现有的应用系统，为用户提供“一点登录、多点漫游”的一站式服务。

系统支持多个应用系统之间的单点登录，即一次登录，多次使用。用户通过身份认证网关认证后，系统认证平台通过 Cookie 机制维护该用户的会话信息，用户登录应用系统时，无需再次认证。极大的简化了用户登录应用系统的步骤，使应用更加流畅。

通过建立系统账号与应用系统账号映射关系，保证网关与应用系统认证一致，实现单点登录。主要有以下几种工作方式：

- 客户端自动代填——系统支持采用客户端控件技术捕获应用系统登录窗口，完成应用系统登录。
- 部署 Filter 插件——对于基于 WEB 的应用系统，在应用系统部署一个 Filter 过滤插件，插件会从网关中获取该用户的从账号信息（用户在应用系统中的账号信息）完成应用系统登录。

另外，管理员可以通过策略配置，授权用户对应用系统的访问。应用入门级控制可以配置以下几种策略：

- 全局默认策略控制——当应用没有配置具体的访问控制策略时，网关通过全局默认策略进行访问控制，全局默认策略的优先级最低。
- 根据用户认证方式控制——可以根据用户认证等级策略控制用户对应用的访问权限。认证等级分为口令认证、数字证书认证、口令+数字证书认证。
- 根据数字证书 DN 规则控制——管理员可以根据用户数字证书，设置 DN 项规则策略，限制某个或某一群组用户对应

用的访问。系统采用黑、白名单的形式设置策略，DN 规则配置灵活，支持通配符。

- 根据时间段规则控制——管理员可以根据时间段规则策略控制某一时间段内，允许访问应用或者禁止访问应用。
- 根据 IP 地址规则控制——管理员可以根据 IP 地址规则策略控制某一 IP 地址或某一 IP 区间段允许访问应用或者禁止访问应用。
- 根据用户名控制——管理员可以根据用户名策略控制某一用户允许或者禁止访问应用。

3.6 数字签名验证服务系统

数字签名验证服务器 (SVS: Sign & Verify Server) 专门提供数字签名服务以及对数据报文验证其数字签名的真实性和有效性，应用于验证用户身份、检验交易凭证。

针对电子公文、电子表格以及其他重要数据的签名、加密需求，工作人员采用证书证书对数据表、资料等数据报文进行电子签名、加盖电子公章，保证信息内容的完整性和不可否认，对价格等部分敏感信息资料可进行加密提交和存储；在电子采购系统中，报价表提交、协议签署等应用中，参与人使用代表其个人或单位的合法有效的数字证书，为相关表格进行电子签名，相关信息内容具有法律效力的有效保证，实现了安全有效的网上报价与网上签约等操作。

签名验证服务器设有专用网络接口管理系统，系统关闭所有

不需要的服务和端口（如 FTP、SSH 等），只保留服务端口，避免外界的攻击。所有管理操作均采用 WEB 方式，操作简单方便。支持多种类型签名数据，支持原文数据签名、文件签名、哈希后签名及 PKCS#7 等格式签名数据的验证。支持多种证书验证方式，支持黑名单验证方式以及 OCSP 验证方式。

同时具有多种开发接口，方便应用的调用。能够输出标准的系统日志，通过标准的 syslog 方式将用户日志发送到指定服务器。系统具有备份和恢复功能，对于系统的数据和配置进行加密。支持双机热备，保证系统的高可用性。

签名验证服务器支持并联、串联、双机并/串联、多种部署方式，可根据实际的建设需要进行灵活部署。

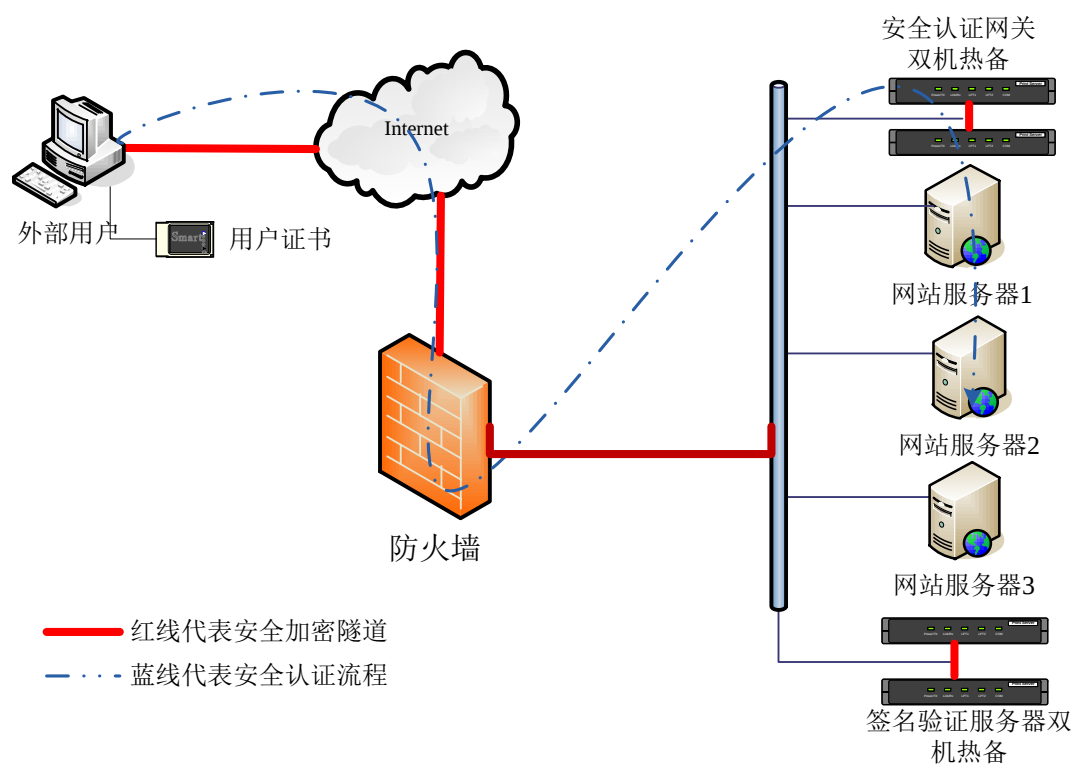


图 11. 部署示意图

3.7 电子签章系统

电子签章将数字签名进行可视化图形转换，为用户提供类似传统印章使用的可视化数字签名应用，例如在电子公文流转过程中，通过电子签章可用于辨识签署者身份，保护数据完整性、防止对数据未经授权的篡改、确保签名行为的不可抵赖，并实现数字签名的直观可视化展现。

电子签章服务基于电子签章系统实现具体功能。电子签章系统具体由电子签章管理系统、数字证书及签章图片、电子签章客户端（网页电子签章）组成：

- 电子签章管理系统：实现电子签章图片的生成、灌制、与证书进行绑定，实现印章生命周期的管理；电子签章管理系统作为电子签章系统的后台管理系统，是整个电子签章系统的核心，完成对每一个电子印章进行整个生命周期的管理，包括电子印章制作、挂失、停用、重新制作、使用控制等全过程的管理；
- 数字证书和签章图片：数字证书和签名图片都保存在证书存储介质中，由证书管理员统一灌制或用户在线进行绑定；
- 电子签章客户端：在本方案中指网页电子签章客户端，实现在应用系统界面上加盖签章、验证签章等功能。

3.8 时间戳服务系统

时间戳服务系统的标准时间从国家天文台标准时间服务器

获取，时间戳服务系统时间戳服务系统主要由时间源服务器，时间戳服务器两部分组成，其中时间戳服务器包括时间服务模块、可信时间戳服务模块、时间戳证据存储服务模块以及密码服务模块。

- 时间服务模块

时间服务模块为可信时间戳服务模块提供可信时间服务，监控并校准时间戳服务模块的时间。时间服务模块通过一个经过认证的、安全的网络连接，向时间戳服务模块提供服务。

- 可信时间戳服务模块

可信时间戳服务模块完成时间戳服务功能。可信时间戳服务模块利用经过时间服务模块同步后的可信时间，利用密码服务系统提供的数字签名，签发可信的时间戳。签发的时间戳格式符合UTC（协调世界时）标准，时间戳服务申请消息格式应该符合RFC3161的规定。

- 时间戳证据存储服务模块

时间戳证据存储服务模块负责保存对应的时间戳服务模块所产生的可信时间戳服务的各类数据信息，以备日后进行审计和举证。时间戳证据存储服务模块需要提供对大容量的时间戳证据信息的存储管理与备份管理功能，并提供对所保存时间戳证据信息的高检索。

- 密码服务模块

密码服务模块为时间戳服务模块加盖的时间戳进行签名服

务，确保可信时间戳服务模块提供的时间戳可信。

可信时间戳服务系统具备：取时功能、对时功能、时间戳服务功能、日志以及证据存储功能、双机热备功能以及管理功能。系统安装部署图如下：

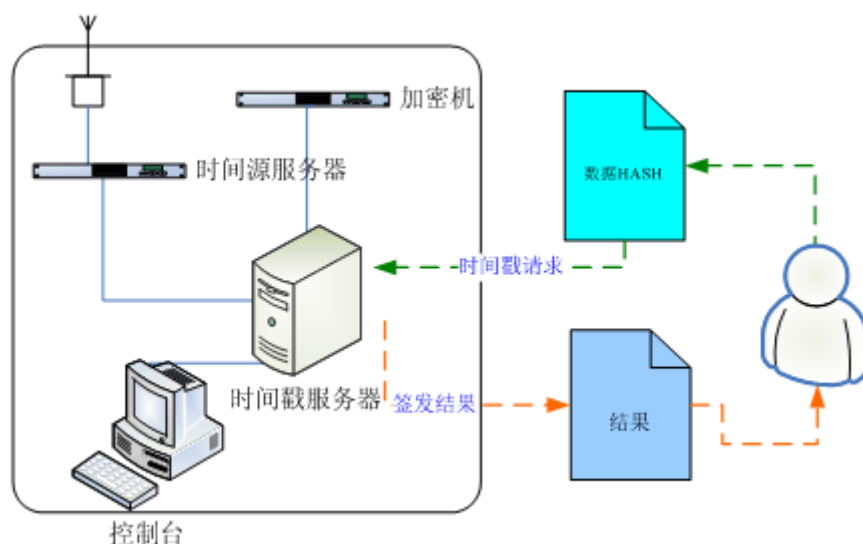


图 12. 时间戳服务器安装部署图

3.9 本地用户注册系统

对于本地用户数量较多，为了满足较高的应用系统技术支撑要求，实现本地用户快捷和高质量的服务需求。证书使用单位可以根据政务CA 证书管理有关规范，建设本地用户注册服务系统（LRA）。LRA 是RA 系统的下级节点，可为本区域的人员提供最终用户提供证书管理服务。

LRA 采用 B/S 模式，负责接收本管辖范围内各种数字证书的请求，并向 RA 系统提出请求，由 RA 系统节点和 CA 系统完成交互，完成证书申请、证书更新、证书作废等请求。

LRA 的管理由 CA 系统和 RA 节点共同负责，省电子认证注册管理中心系统负责 LRA 建设的审批和 LRA 系统的日常运维管理，如 LRA 的权限设置等。LRA 需要和省电子认证注册管理中心签署相应的协议，代表省电子认证注册管理中心在本部门提供证书相关服务，担负相应的责任。

- 系统功能

提供基本的证书信息管理服务，包括：注册、签发审核、证书签发、更新申请、更新审核、证书更新、废除申请、废除审核、证书废除、重发申请、重发审核、证书重发和信息注销。提供基本的证书辅助管理功能包括查询/统计/归档等。

- 系统部署结构设计

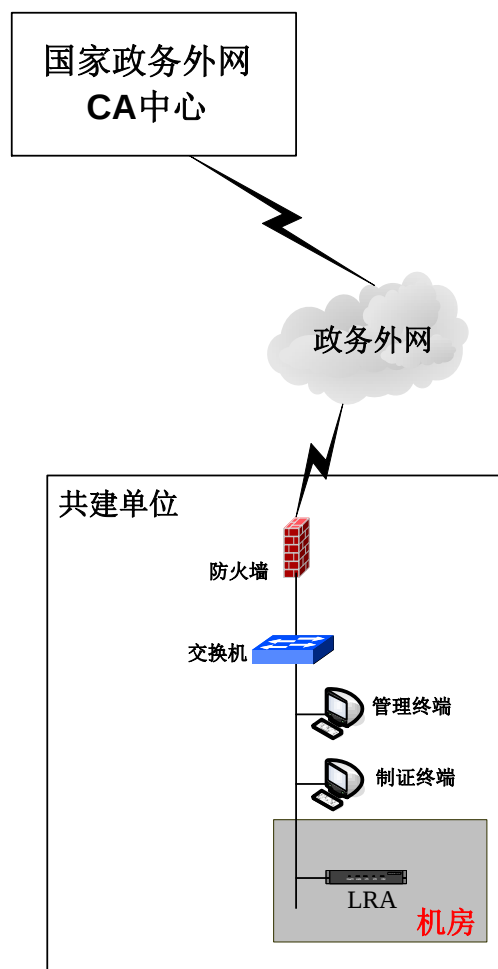


图 13. LRA 系统部署图

4 电子认证应用案例

政务CA为部署在国家电子政务外网和互联网上的业务应用提供跨部门、跨区域电子认证服务。据不完全统计，截至2013年底，已为21个部委、17个省市的业务应用提供了电子认证服务。主要有四类应用：

1、安全接入政务外网。国务院扶贫开发领导小组办公室、中纪委监察部、中华全国妇女联合会、中国民主建国会等中央政务部门使

用政务 CA 数字证书实现互联网安全接入政务外网，保障数据传输安全。

2、**中央政务业务系统身份认证与数字签名。**国务院应急工作办公室全国应急信息平台、国家人口基础信息库、国家自然资源和地理空间基础信息库、国家发展改革委“12358”全国价格举报管理信息系统、国家环境保护部环境信息与统计能力建设项目、国务院机关事务管理局人防办信息系统、国家安全生产监察总局安全生产监管信息化工程、国家审计署金审工程和中华全国总工会等中央政务业务系统应用了政务 CA 数字证书，保障业务系统应用安全

3、**地方政务业务系统身份认证与数字签名。**为地方政务部门提供业务系统数字证书应用，如山东事业单位监督管理信息系统、四川省行政权力依法规范公开运行平台、安徽省财政采购平台、陕西省公共信用信息交换平台和大连市电子政务平台、贵州省遵义市政府网上办公系统等。

4、**移动电子政务应用。**为解决移动电子政务面临的安全和标准化问题，为各级政务部门的移动电子政务应用创造一套标准化、安全的移动应用环境，政务 CA 联合国内知名平板电脑厂商和基础电信运营商，将政务 CA 数字证书内置于移动智能终端，集成开发了移动环境下达到信息安全等级保护三级的“安全政务本”，为非涉密业务系统提供了电子政务移动应用平台。

政务 CA 与中华印章协会合作，将数字证书内置于电子印章，开发了便于携带、方便应用的物电一体化的印章产品。

主要应用案例有：

● 国家审计署应用

数字认证以审计机关局域网为单位实现，其中中央审计机关局域网 19 个（审计署机关和 18 个特派办），省级审计机关局域网 37 个，地市级审计机关局域网 330 个。

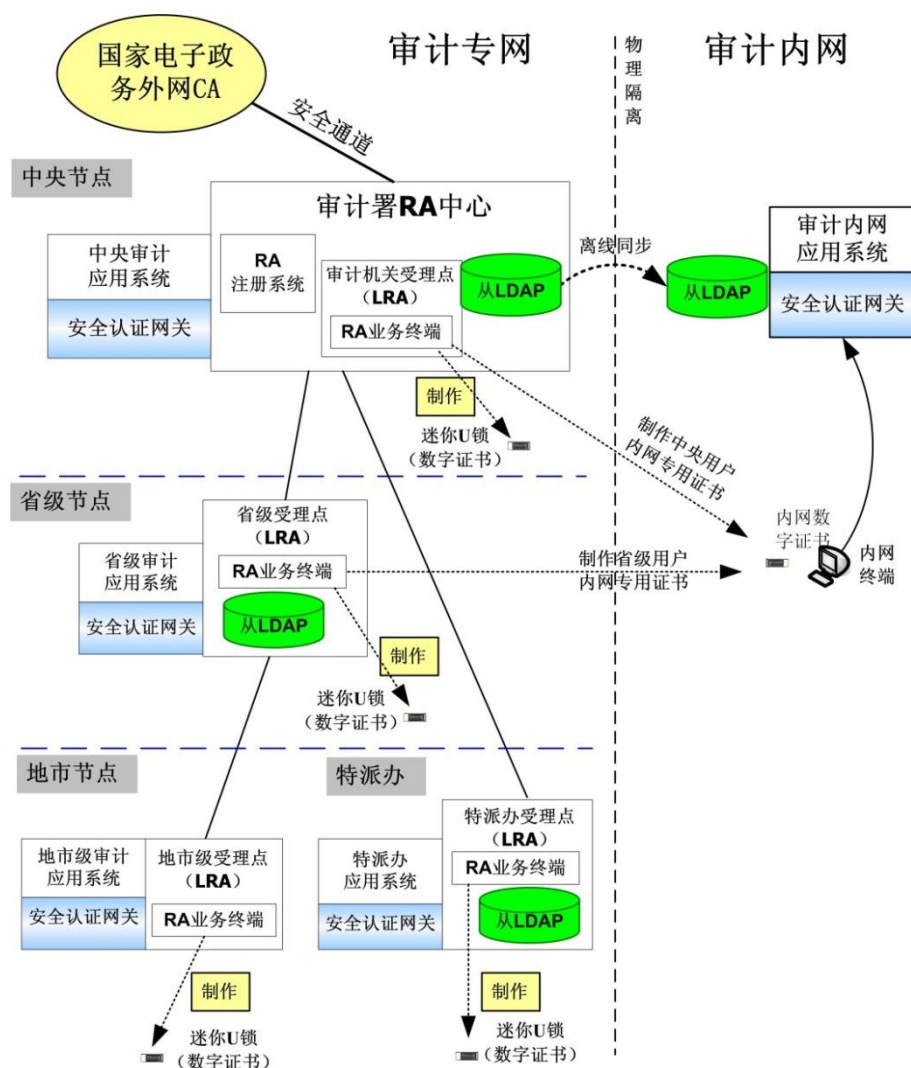


图 14. 审计署建设部署图

● 国家环保部应用

作为国家环保部的信息化安全基础支撑设施，为信息化提供统一的身份认证支撑服务，后续各个司局建设的应用系统均会采

用本次建设完成的身份认证体系，保证每个用户手里只有一个KEY，实现“一证通”。

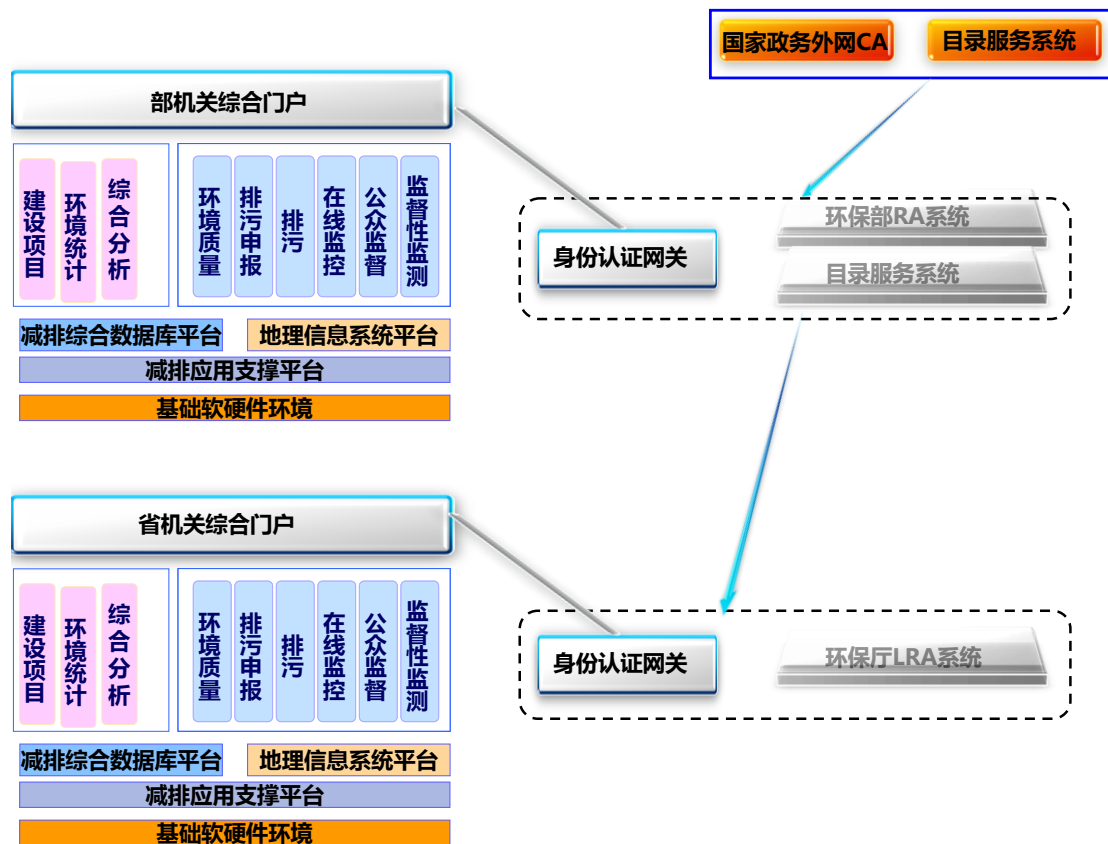


图 15. 环保部建设部署图

● 国务院扶贫办应用

农村最低生活保障和开发式扶贫是目前我国扶贫事业的两项重要制度。农村最低生活保障制度和扶贫开发政策有效衔接的主要含义，就是把对农村低收入人口实施的最低生活保障制度和扶贫开发政策有效衔接起来，实现“应保尽保、应扶尽扶”。

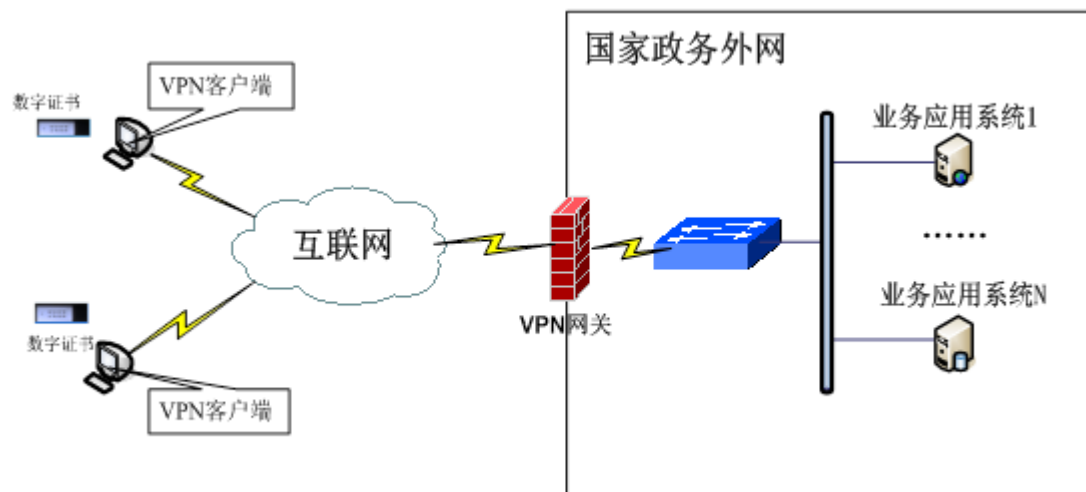


图 16. 扶贫办拓扑图

● 全国总工会应用

主要用于全国工会统计调查系统利用网络完成统计年报的数据报送。软件的使用者为全国各级总工会负责统计调查的工会干部。这些工会干部只能使用政务 CA 发放的数字证书登录统计年报数据处理系统，实现基于数字证书的身份认证和信息加密。

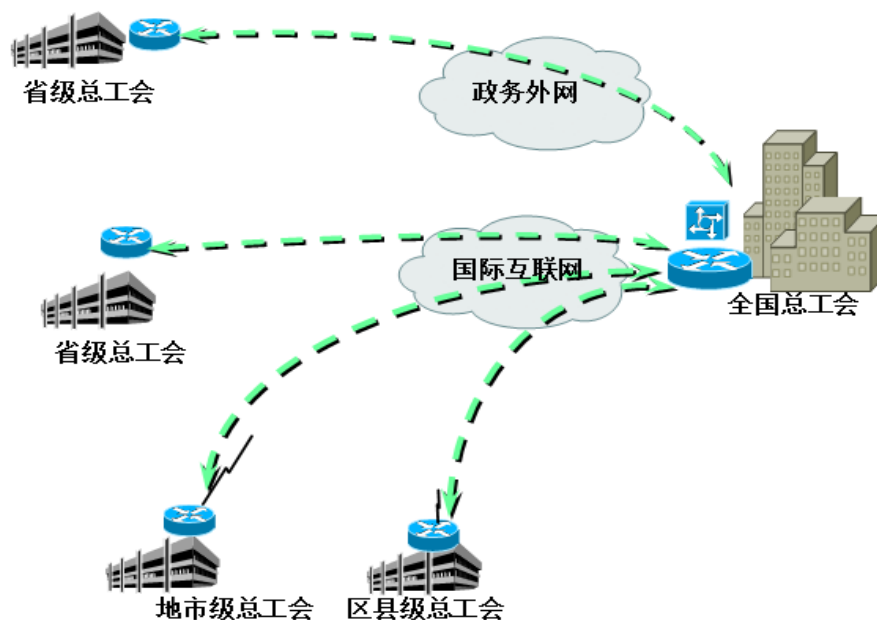


图 17. 全国总工会部署图

● 国务院应急平台

国务院应急平台依托政务外网连接了 26 个中央政务部门和 37 个地方的应急平台。用以应对抗震救灾等突发事件。主要业务类型包括视频、图像、语音、数据和移动通讯等。

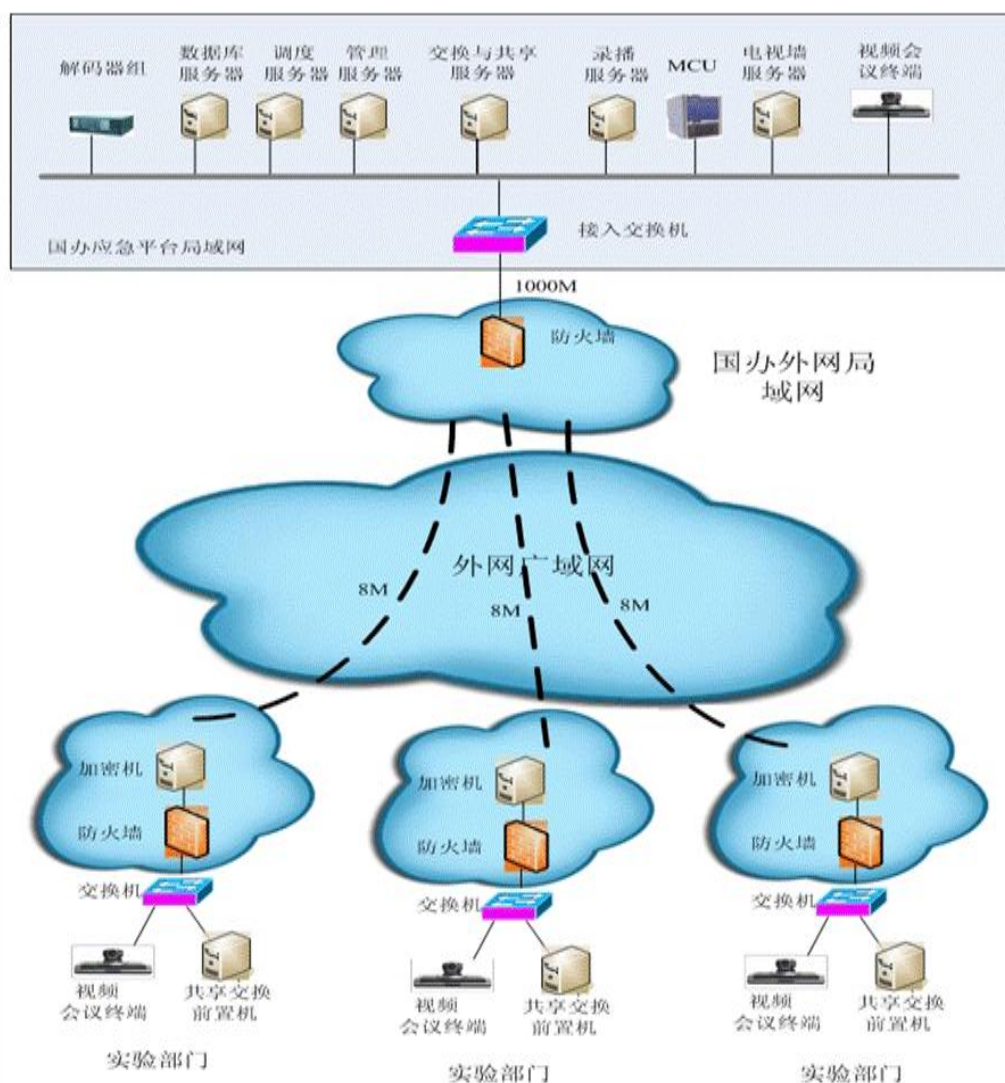


图 18. 国务院应急平台部署图

● 中纪委监察纠风系统

纠风之窗网站受理网上信访举报，用户使用政务外网数字证书登录系统。监察部人员可在信息管理系统办理或者向地方纠风单位转办、督办案件。办结结果通过纠风之窗网站向网民反馈。

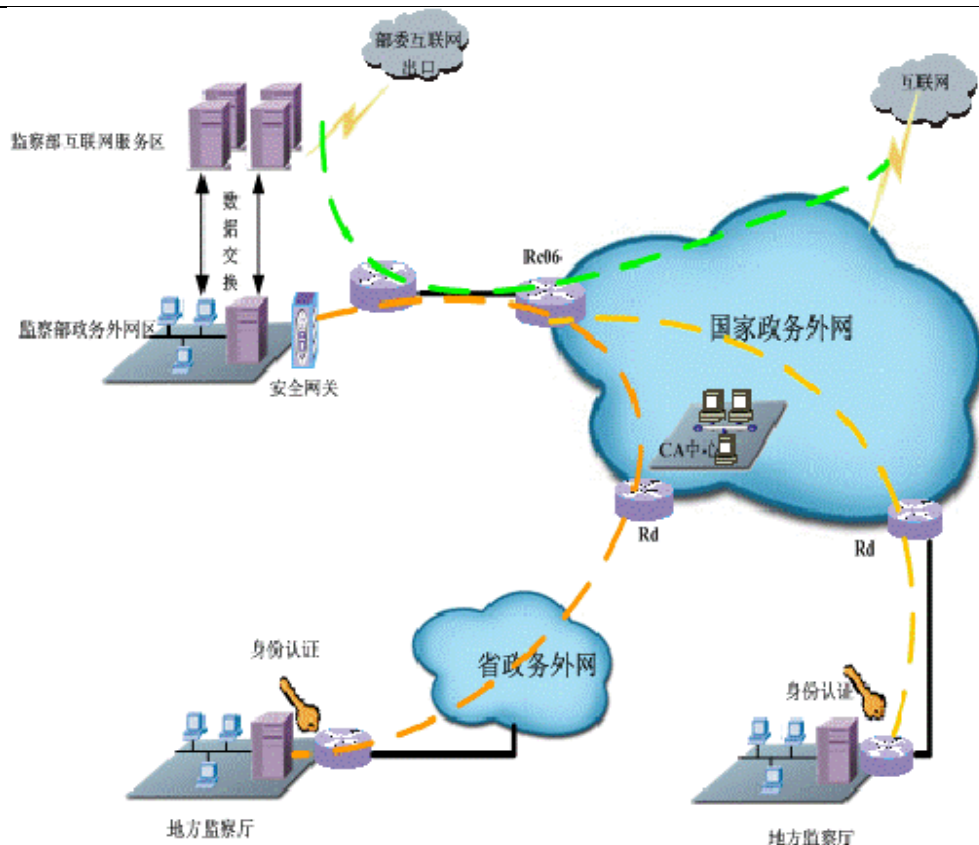


图 19. 纠风系统部署图

● 最高检察院案件信息公开系统

案件信息公开系统主要包含社会用户、检察机关用户和系统管理员用户三类人员，为保障系统访问安全，后两类用户设计使用数字证书进行系统登录和访问，中央到县四级分布，共有用户1万人。此次认证服务系统建设主要包含身份认证网关的建设和1万用户的数字证书制作发放。

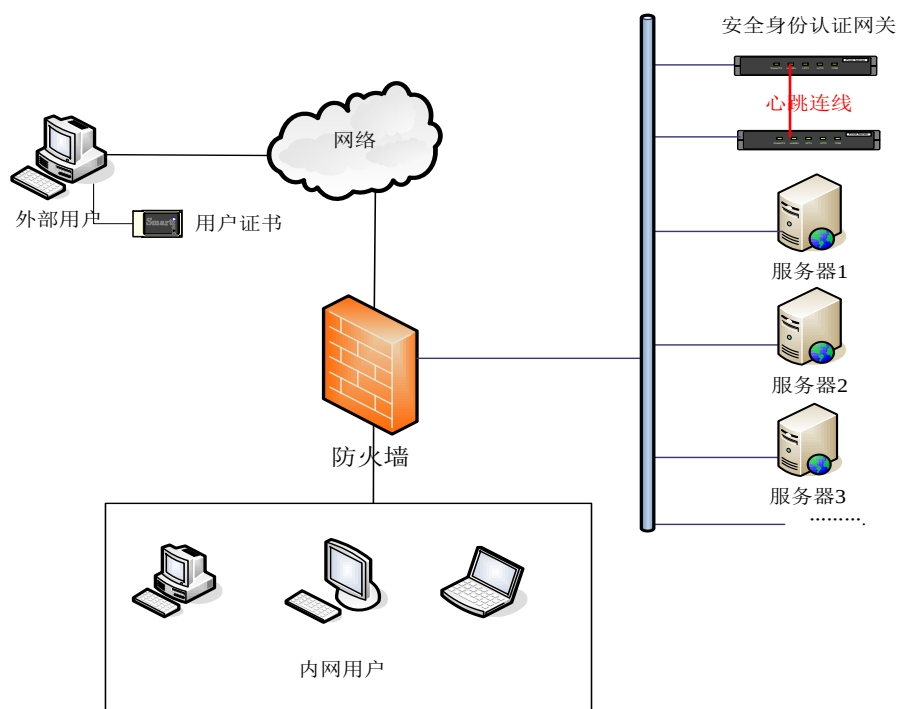


图 20. 部署示意图

● 国家安全生产监督管理局应用系统

安全生产监管信息化工程是“十二五”国家政务信息化工程建设项目之一，按照中央有关文件精神 and 《关于加强和完善国家电子政务工程建设管理的意见》（发改高技〔2013〕266 号）要求，使用国家电子政务外网的信任服务设施，实现跨部门、跨区域的业务应用，为全国用户提供用户身份认证。部署示意图同上。

● 中央国家机关人民防空办公室

随着中央国家机关人防信息化推进，国管局人防办已建设中央国家机关人防工程相关的若干信息化系统，包括人防数据采集系统、人防审批管理系统、人防互联网门户等。为保障各系统安全，将现有身份认证系统进行改造接入政务外网政务 CA 的数字证书服务。部署示意图同上。

● 12358 全国价格举报管理信息系统

该信息系统集中部署在国家电子政务外网中央公用网络区，各级价格主管部门通过国家电子政务外网连接，并访问中央系统。未接入外网或移动接入的单位及个人可通过该信息系统部署在中央的 SSL VPN 网关或各省的 VPN 网关接入外网，访问系统。按照要求，国家电子政务外网数字证书使用在两个场景中，一个作为信息系统的身份认证，所有访问者都需要使用。另一个作为 VPN 接入认证。

● 应用拓展——《安全政务本》

与华为、联想、中兴、一人一本等平板电脑厂商和中国电信、中国移动、中国联通等电信运营商合作，开发了达到等级保护三级安全水平的《安全政务本》系统，应用于各级政务部门的非保密移动电子政务业务。“政务 CA” 数字证书以 TF 密码卡的形式内置于 PAD 或智能手机中，开创了证书应用推广的新模式。

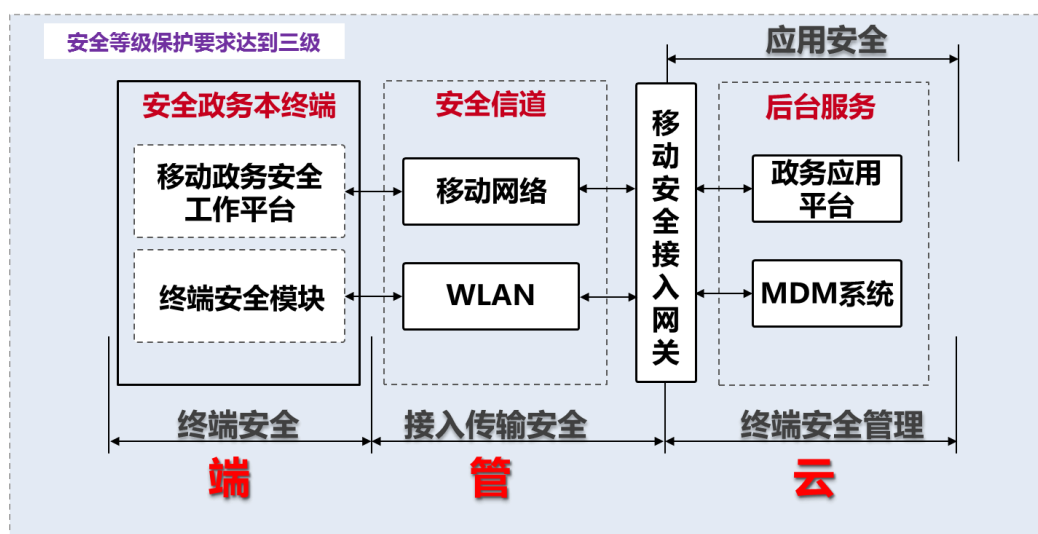


图 21. 安全政务本系统架构图

附件 1. 涉及主要产品

1. 身份认证网关

身份认证网关功能如下表：

功能	说明
证书认证	
单双向认证选择功能	系统可以设置是否需要用户提交用户证书
动态黑名单功能	系统可自动更新黑名单、动态更新，不需要重启服务 支持 LDAP、HTTP、手工上传等多种方式更新 支持 B64、DER 等多种格式
多站点证书功能	系统可以拥有多个站点证书，不同的服务可以拥有不同的站点证书
多证书链功能	一个 SSL 服务中可同时配置多条证书链，验证不同 CA 的用户证书
多种证书支持功能	支持格尔、CFCA、SHECA 及多数省级 CA 中心数字证书
应用支持	
多服务功能	系统可以创建多个 SSL 服务，保护不同的应用服务，也可以采用同一个 SSL 服务保护多个应用服务(需客户端)
支持应用重定向功能	在有防火墙 NAT 映射的情况下正常访问有重定向的网站
信息传送功能	系统通过 URL，HTTP header，cookie 多种方式将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息
后台应用负载功能	一个认证服务可以对后端多台应用服务器进行负载均衡

信息统计	系统能够对用户连接数、应用访问情况，系统资源占用等信息进行详细统计，为更好了解应用及调节资源提供基础
错误重定向	系统对于认证错误可以重定向到用户指定页面，增强友好性
国密算法支持	
	支持扩展国密非对称算法 SM2
	支持扩展国密对称算法 SM1
	支持扩展国密杂凑算法 SM3。
系统管理	
管理员三权分立	提供管理员三权分立功能，不同的管理员负责不同的功能配置，相互制约。
系统备份恢复功能	系统可以备份当前 SSL 的所有配置，保证系统瘫痪时的快速恢复
日志发送功能	系统将日志以 SYSLOG 的方式发送到指定服务器。
系统在线升级	系统支持 Web 方式的系统升级
性能检测功能	系统支持对 CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位
可用性	
双机热备功能	高可靠性
自负载均衡	系统具有集群功能，可以对多台设备进行负载
网卡热备功能	可以对两块网卡进行冗余配置，当一块网卡失效后，另一块网卡自动生效

网卡负载功能	可以对两块网卡进行绑定聚合，将请求和流量负载到两块网卡上
易用性	
管理员易于操作	系统所有管理操作都通过 web 方式进行，方便使用
用户的良好体验	系统可以为终端用户提供良好的错误提示，如证书过期，证书未生效，证书已经作废等信息，不会显示“此页无法显示”令用户不知所措的页面

身份认证网关外网定制型性能参数如下表：

	E2010 政务外网定制型	E2020 政务外网定制型	E2040 政务外网定制型	G4020 政务外网定制型	G4040 政务外网定制型
设备高度	1u	1u	1u	2u	2u
网络接口	4*1000M	4*1000M	4*1000M	4*1000M (扩展 4 电口或者 2 光口)	4*1000M (扩展 4 电口或者 2 光口)
最大新建连接数	60 次/秒	160 次/秒	1000 次/秒	2500 次/秒	4000 次/秒
每秒完成交易数 (TPS)	1000 次/秒	3000 次/秒	5000 次/秒	10000 次/秒	25000 次/秒
最大并发连接数	400	800	1500	2500	5500
最大流量	50Mbps	120Mbps	250Mbps	680Mbps	850Mbps

2. 数字签名验证服务器

数字签名系统功能如下表：

功能	说明
数据签名功能	提供普通格式/P7 attach/P7 detach 等多种格式的数字签名功能

签名验证功能	提供普通格式/P7 attach/P7 detach 等多种格式的数字签名验证功能
文件签名功能	对文件提供数字签名功能（在 API 中计算摘要）
文件验证签名功能	对文件提供数字签名验证功能（在 API 中计算摘要）
证书有效性验证功能	提供黑名单/在线证书验证等多种方式的证书有效性验证
动态黑名单功能	系统可以自动更新黑名单、动态更新，不需要重新启动服务
多签名证书功能	可同时配置多张签名证书，由调用者选择使用哪张进行签名，并可对单张签名证书设定 PIN 保护
多证书链功能	可同时配置多条证书链，验证不同 CA 的用户证书
获取证书信息功能	提供证书解析功能，获取证书中的任意主题信息以及扩展项信息
多种证书支持功能	支持格尔、CFCA、SHECA 及多数省级 CA 中心数字证书
系统备份恢复功能	系统可以备份当前所有配置，保证系统瘫痪时的快速恢复
日志发送功能	系统将日志以 SYSLOG 的方式发送到指定服务器。
双机热备功能	高可靠性
多种开发接口支持	客户端提供 C 开发 API，COM 方式 API，Java 开发 API

数字签名验证服务器性能参数表如下：

	SVS-E2010 政务外网定制型	SVS-E2020 政务外网定制型
设备高度	1u	1u
网络接口	4*1000M	4*1000M
签名	100 次/秒	150 次/秒
验签	300 次/秒	500 次/秒
支持算法	RSA、SM2	RSA、SM2

3. 时间戳服务系统

时间戳服务系统基本功能如下表：

功能类别	功能名称
服务功能	验证时间戳请求
	通过时间获取接口获取标准时间
	签发时间戳
	接收时间戳请求和返回时间戳响应
日志服务	WEB 方式管理功能
	页面生成证书请求
	导入签发的证书
	启动和停止服务
	配置时间服务器相关参数
	时间证据信息 Syslog 方式发出，可配置接收服务器 IP
	可以配置加密设备
日志服务	系统运行日志查询
	运行日志定期清除
	支持 Syslog 方式向外发送日志
客户端 API	提供用户数据 hash 函数，支持 SHA1 算法等
	建立时间戳请求函数
	提供请求时间戳函数（发送时间戳请求）
	提供验证时间戳函数（对用户的时间戳进行验证）
	解析时间戳应答函数
	提供 C++ 和 JAVA 两套接口 API

4. 本地用户注册系统

本地用户注册系统基本功能如下：

功能	说明	功能类型
证书管理功能		
用户信息注册	提供注册用户信息，包括批量注册功能	基本功能
用户信息查询	提供查询用户信息，可根据相关条件进行筛选查询	基本功能

用户证书签发	提供用户证书签发功能，允许将用户证书安装到 USBKEY	基本功能
用户证书更新	提供用户证书信息更新功能，允许修改用户证书信息。	基本功能
用户证书废除	提供用户证书废除功能，允许废除用户证书。	基本功能
用户信息注销	提供用户信息注销功能，允许注销已经废除后的用户信息。	基本功能
应用支持		
通过 IE 浏览器访问管理	支持微软 IE6.0 以上版本的浏览器进行管理	基本功能
支持将证书安装到 USBKEY	支持将证书签发到所有运行标准 CSP 接口的 USBKEY	基本功能
特色功能		
系统性能本地监控	系统能够对用户连接数、应用访问情况，系统资源占用等信息进行详细监控，为更好了解应用及调节资源提供基础	基本功能
系统状态远程监控	系统支持通过 SNMP 方式将设备运行情况发送到第三方监控系统	基本功能
设备管理员三权分立	支持将设备的管理模式设置为三权分立模式	基本功能
支持远程重启系统	可在远程通过 web 管理界面重启系统	基本功能
HTTPS 登录系统	LRA 系统管理控制台和业务操作界面，都使用 HTTPS 协议进行通讯，保障数据传输安全	基本功能

有效认证 LRA 操作员身份	LRA 系统自动防止 LRA 操作员非法登录，外地 LRA 系统的操作员无法登录本地 LRA 系统	基本功能
LRA 系统业务权限统一由 RA 中心分发	由 RA 中心为各地 LRA 系统进行业务功能授权，业务授权得到统一管理	基本功能
对证书管理的审核权限由 RA 中心控制	在 LRA 系统中进行业务操作，都需要先通过 RA 中心审核。	基本功能
LRA 系统的站点证书统一由国家信息中心管理	LRA 系统的站点证书统一由国家信息中心管理	基本功能
系统管理		
系统备份恢复功能	系统可以备份所有配置信息，保证系统瘫痪时的快速恢复	基本功能
恢复出厂设置功能	系统具有恢复默认设置功能，方便使用	基本功能
日志发送功能	系统将日志以 SYSLOG 的方式发送到指定服务器。	基本功能
系统在线升级	系统支持 Web 方式的系统升级	基本功能
性能监测功能	系统支持对 CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位	基本功能
易用性		
管理员易于操作	系统所有管理操作都通过 web 方式进行，方便使用	基本功能
用户的良好体验	业务操作步骤简洁，注册、签发、更新、废除等业务操作步骤简单明确。	基本功能

本地用户注册系统采用专用网络硬件设备，参数如下：

	政务 I 型
设备高度	1U
网络接口	4*100M
最大发证数量	无限制
每秒发证速度	5 张/秒