无线电管理应用安全平台体系架构及应用规范

目 录

1.范围 1
2. 规范性引用文件 1
3. 符号和缩略语 2
4. 术语和定义 2
5. 概述 4
5.1 背景 4
5.2 主要目的 5
5.3 主要原则 5
6. 总体技术框架 7
6.1 总体架构图 7
6.3 区域逻辑结构 9
7. 应用安全平台建设规范 11
7.1 CA 系统建设规范 11
7.2 4A 系统建设规范 13
8. 应用系统安全规范 16
8.1 基于 CA 系统建设规范 16
8.2 基于 4A 系统建设规范 16
附录 A 18
附录 B 19
附录 C 20
附录 D 21
附录 E 25
附录 F 29
附录 G 30
附录 H 32

1.范围

本规范规定了无线电管理一体化平台建设信息系统涉及的有关统一目录管理、单点登录、统一身份管理、统一认证、授权及审计管理等的应用安全体系建设的原则和方法，适用于全国各级无线电管理机构和全国无线电管理信息系统中的应用安全平台及应用系统、网络安全传输设备及其运行和管理软件等的开发和实施单位。

本规范的内容范围是是基于无线电管理一体化平台建设信息系统涉及的有关统一目录管理、单点登录、统一身份管理、统一认证、授权及审计管理等的应用安全体系建设的指导性规范文档，包括以下五个部分：

概述，介绍了应用安全平台建设的背景、目的、原则。

总体框架说明，从总体框架图、应用安全平台逻辑结构、区域逻辑结构三个方面详细阐述了应用安全平台内部组成、应用安全平台与一体化平台、应用安全平台与应用系统以及国家中心和各省中心的应用安全平台之间的关系。

应用安全平台建设规范，对应用安全平台的两大组成部分（CA 系统及 4A 系统）的建设规范分别进行了详细说明。

应用系统建设规范，对应用系统在基于应用安全平台进行系统建设时所要遵循的安全规范进行详细阐述。

附录，包括证书申请使用规范、区域代码表等八个附录。

2.规范性引用文件

全国无线电管理信息系统应用安全规范

无线电管理一体化平台体系架构及应用规范

3.符号和缩略语

CA	数字证书签发机构	Certification Authority
AAA	AAA 为用户提供统一的身份认证、资源访问权限控制和日志审计服务。本文档中的 AAA 是指全国无线电管理机构原有的 AAA 系统	Authentication、Authorization、Auditing
4A	4A 为用户提供账号管理、身份认证、资源访问权限控制和日志审计的服务	Account、Authentication、Authorization、Auditing
LDAP	轻量目录存取协议，它是一个快速增长的对通用目录信息进行存取的技术。本文档中的 LDAP 是指用户信息库	Lightweight Directory Access Protocol
LRA	本地注册机构	Local Registration Authority
OCSP	在线证书状态协议	Certificate Status Protocol
CryptpAPI	为应用程序开发者提供 Windows 环境下使用加密、验证等安全服务时的标准加密接口	Cryptography Application Programming Interface
RADIUS	远程用户拨号认证系统	Remote Authentication Dial In User Service
Filter	过滤器	

4.术语和定义

4.1. 国家中心用户信息库

国家中心用户信息库包含了全国无线电管理机构所有用户的身份信息、证书信息和组织机构信息，存储在国家中心的 4A 系统中。

4.2. 省级用户信息库

省级用户信息库指各省无线电管理机构的用户身份信息、证书信息和组织机构信息，存储在各省的 4A 系统中。

4.3. 用户身份库

用户身份库指存储 4A 系统相关的账号、权限和审计等信息。

4.4. 身份管理

身份管理是对用户身份的创建、修改、迁移、冻结、删除和同步等操作的管理。

4.5. 账号

应用系统中用于登录的用户名叫做账号。

4.6. 审计管理

审计管理是对用户的登录和操作等行为进行记录，查询和系统分析的过程。

4.7. 数字证书

数字证书是网络通讯中标志通信各方身份信息的一系列数据，提供了一种验证身份的方式，其作用类似于身份证。它由权威机构--CA 机构颁发，在相互通信中用它来识别双方的身份。

4.8. 单点登录

单点登录是指“登录一次，便可访问多个系统”。

4.9. 证书注销列表

证书注销列表是在证书有效期之内，CA 签发的终止使用证书的信息。

4.10. 票据

用户认证通过后，4A 系统的认证服务器给用户签发一个用户认证通过凭证，这个凭证就是票据。

4.11. 互信中心服务

互信中心服务由国家中心 4A 系统提供，为跨域访问的用户提供票据验证的服务。

4.12. 入口级授权

入口级授权是指用户是否有权访问应用系统，而对用户访问应用系统的具体内容不做控制。

4.13. 细粒度授权

细粒度授权是指对用户访问应用系统的具体内容，例如：菜单、功能模块、URL 等进行授权。

5.概述

5.1 背景

全国无线电管理信息系统经过“十五”、“十一五”建设，已经初具规模，先后建设了频率台站、天馈线、设备检测、办公 OA 等应用系统。在信息安全基础建设方面，建设了以 CA 系统和 AAA 系统为基础的应用安全平台，提供了基于 USBKey 数字证书的用户身份认证，业务单点登录访问、权限控制、操作审计等功能，并制定下发了《全国无线电管理信息系统应用安全规范》（信无函[2007]17 号）。这些应用系统和信息安全基础设施的建设，很好满足了全国无线电管理机构信息化和信息安全的建设需要，为无线电管理工作起到了有力的业务支撑和安全支撑，并为下一阶段全国无线电管理信息化建设打下了坚实的基础。

但目前，全国无线电管理信息系统建设基本以应用系统为单位进行建设的，由于缺乏全局规划、缺乏统一的标准体系，每个系统受自身格局所限，形成了一个个的孤岛，系统之间衔接困难，系统的可扩展性差，存在着孤立的应用系统、中断的业务流程、分散的数据碎片和低效的信息资源等问题，难以满足业务不断变化和发展需要；而在安全建设方面，原有的 AAA 系统存在部分技术过时、对跨域访问的支持功能有限以及与应用系统全面整合困难等，而无法满足无线电管理信息系统安全建设的变化和进一步发展需要。因此，迫切需要一个统一的平台来合理整合无线电管理的信息资源及应用，实现全局信息资源共享及人员协作。与之相适应，对原有的应用安全平台（CA 和 AAA 系统）及安全规范需要升级，升级后的应用安全平台是无线电管理一体化平台的重要组成部分，对一体化平台及各类无线电管理应用系统提供用户身份、接入认证、单点登录、统一授权、日志审计和跨域访问等基础支撑服务。

为了保障应用安全平台顺利升级成功，必须对应用安全平台进行统一的设计和验证，实现统一的技术架构、统一的目录结构、规范的目录命名、统一的目录同步机制、统一的应用接入方式、规范的分级授权管理模式，形成相应的建设指导性规范文件。

5.2 主要目的

本文档作为全国无线电管理信息系统应用安全平台（以下简称“应用安全平台”）及其上应用的建设标准规范，一方面是规范无线电管理应用安全平台的升级，另一方面是规范无线电管理应用系统的安全建设，具体内容包括：

a) 规范应用安全平台的系统架构，满足“两级架构，多级管理”的总体要求；

b) 规范应用安全平台的目录实体命名编码规则；

c) 规范应用安全平台的统一认证及单点登录机制；

d) 规范应用安全平台的国家中心到各省分中心跨域认证机制；

e) 规范应用安全平台的统一授权机制；

f) 规范应用安全平台的统一审计机制；

g) 规范应用安全平台的应用系统集成接口。

5.3 主要原则

应用安全平台及应用的建设遵循如下原则：

a) 统一性原则

应用安全平台的建设必须遵循统一原则，即统一规划、统一设计、统一验证和统一标准的原则。

b) 实用性

系统的建设将遵循实用性的原则，即切实解决全国无线电管理信息系统的应用安全需要，尽量采用简单明了的方案以降低系统成本。

c) 利旧原则

应用安全平台的建设遵循利旧原则，合理考虑节约系统建设成本，在现有应用安全平台的基础上进行升级改造。

d) 先进性原则

应用安全平台的体系架构要采用国际先进的技术路线，基于先进的系统架构，结合国内外成

功案例的设计经验，从根本上保证系统运行的高效、稳定、安全。

e) 易扩展性原则

应用安全平台的体系架构需要考虑现有的应用系统和未来需要建设的应用系统，以便保证整个系统的不断发展。

f) 高可用性原则

应用安全平台的技术架构必须要着重考虑系统运行的稳定性，对设计中的关键组件应灵活采用双机热备等高可用性方案，并提供较完善的备份恢复策略，较好地解决单点故障和系统灾难问题。

g) 安全性原则

应用安全平台的技术架构必须要充分考虑影响系统安全的各种因素，在数据通信、物理部署等多个层面上落实系统的安全性原则。

h) 标准化原则

应用安全平台在架构、服务、数据和接口等多个层面上形成各级无线电管理机构建设的标准。

i) 平滑过渡原则

应用安全平台的设计优先保证对核心需求、核心系统的实现，在此基础上渐次扩展覆盖范围，尽量减少因系统建设对最终用户的影响。

6. 总体技术框架

6.1 总体架构图

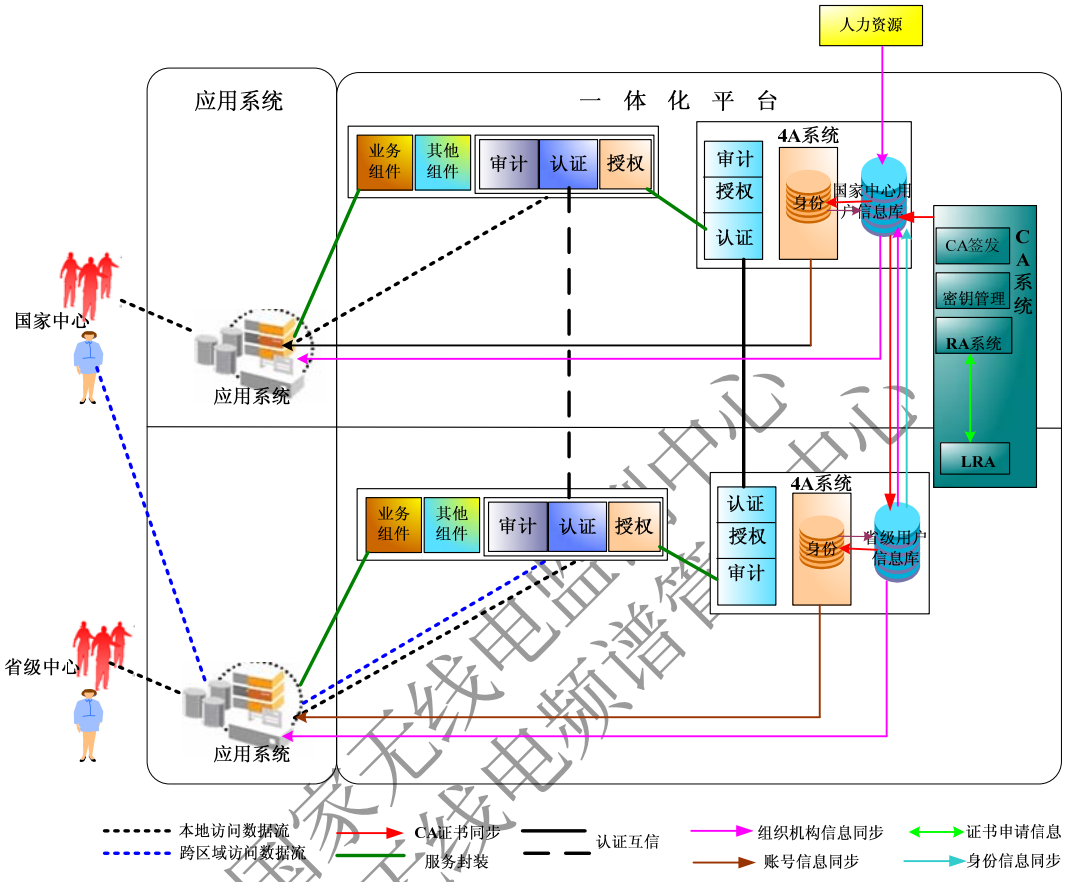

图 6-1：总体架构图

应用安全平台是无线电管理一体化平台的组成部分之一，应用安全平台由 CA 系统和 4A 系统两部分组成。CA 系统已由国家中心建设完成，主要为全国各级无线电管理机构的所有用户进行证书申请、审核和签发等，各地无线电管理机构主要负责向国家中心提交证书申请信息。4A 需要国家中心和各省分别建设，4A 系统提供统一的用户管理、认证管理、授权管理、审计管理和组织机构管理等，国家中心的 4A 系统还提供一个互信中心服务，为跨域访问的用户提供票据的验证服务。应用安全平台的各个系统之间、应用安全平台与一体化平台之间的逻辑关系如图 6-1 所示。

6.2 应用安全平台逻辑结构

应用安全平台是由 CA 系统和 4A 系统两部分组成。CA 系统提供数字证书、签名和加密

等服务；4A 系统提供统一的用户身份管理、身份认证、授权管理、审计管理和组织机构管理等服务。

6.2.1 CA 与 4A 关系

a) CA 系统为 4A 系统的身份认证服务提供证书

CA 系统为全国无线电管理机构的所有用户签发数字证书，4A 系统为用户提供统一的强身份认证。

b) 4A 系统从 CA 系统同步用户身份信息

国家中心及各省中心的 4A 系统均需要从国家中心用户信息库中读取用户证书信息，并基于证书信息生成用户账号信息。读取接口参见附录 C。

6.2.2 CA 与一体化平台的关系

CA 系统作为一体化平台的一部分，为一体化平台提供数字证书。

6.2.3 4A 与一体化平台关系

4A 系统提供的认证管理、授权管理等功能被封装并注册到一体化平台的服务总线上，为用户访问应用系统提供统一的认证、授权等服务。

6.2.4 CA 与应用系统关系

CA 系统提供数字证书，证书格式采用 X.509 标准，满足应用系统的强身份认证；还可以为应用系统提供数字签名、信息完整性和机密性等服务。CA 证书的开发接口参见附录 G。

6.2.5 4A 系统与应用系统

a) 4A 系统提供账号服务

4A 系统为应用系统提供统一的账号管理服务，新建设的应用系统不用建设账号信息，直接接受 4A 系统推送的账号信息；对于已建设的有账号的应用系统，4A 系统需要收集账号信息，存储在 4A 系统的身份信息库中，并与 4A 系统基于证书生成的账号进行映射，以便于实现单点登录。

b) 4A 提供认证授权和审计服务

4A 系统为应用系统提供统一的用户管理、认证管理、授权管理和审计管理等功能。

c) 4A 提供组织机构信息

应用系统如果需要组织机构信息，可以直接从 4A 系统的用户信息库中读取。

6.3 区域逻辑结构

6.3.1 国家中心与各省之间

6.3.1.1 CA 系统

CA 系统已由国家中心统一建设，各省只需通过部署的远程注册系统，将用户注册信息提交至国家中心进行审核，CA 系统审核通过后为用户签发数字证书。证书申请规范详见附录 A。

6.3.1.2 4A 系统

6.3.1.2.1 身份管理

国家中心建立国家中心用户信息库，除了存储国家中心的组织机构信息、用户身份信息和全国的用户证书数据外，还将存储由各省中心上报来的组织机构和用户身份数据，今后将作为全网范围内最完整、准确的中央身份库。

各省中心建立本省范围内的省级用户信息库，存储本省范围内的组织机构信息、用户身份信息和用户证书数据。其中用户证书数据需从国家中心用户信息库中读取；用户信息和组织机构信息如有变动，需提交给国家中心，具体如下：

各省的 4A 系统从国家中心用户信息库中同步本省所有用户证书信息，全国无线电管理机构中的每个用户的唯一编码是由 4 位国标“区域代码”和“用户编号”组成；各省只能同步具有本省区域代码标识的用户证书信息。例如：湖北省只能同步用户编码为“4200XXXX”的用户证书信息。具体的编码规范详见附录 B。

各省 4A 系统需要从国家中心用户信息库中基于证书读取接口（详见附录 C）读取各省用户证书信息，基于证书信息生成用户身份信息，并按照用户身份信息模板（详见附录 D.3 的用户信息模板）将用户身份信息提交至国家中心，由国家中心人员审核后，同步至国家中心用户信息库中。各省用户身份信息如有变动，各省需将变动的信息通过模板（详见附录 D.3 提报信息模板）提交至国家中心，由国家中心将人员变动信息审核通过后，同步至国家中心用户信息库中。

各省中心按照用户组织机构信息模板（详见附录 D.3 的组织机构信息模板），将本省用

户组织机构信息提交至国家中心，如果人员岗位、部门等信息有变动，各省将变动的信息通过模板（详见附录 D.3 提报信息模板）提交至国家中心，由国家中心将人员变动信息审核通过后，同步至国家中心用户信息库中。

各省如有用户需要跨域访问国家中心资源，用户身份信息同步应遵循如下流程：

a) 首先由本省的管理员将本省需要进行跨域访问的用户进行统计，向国家中心的管理员提交申请；

b) 国家中心管理员审核通过后，从国家中心库中同步跨域访问用户的身份信息。

6.3.1.2.2 身份认证

如果某省有用户需要跨域访问国家中心资源，本省的 4A 系统的身份认证服务与国家中心的身份认证服务必须互信，系统时间必须保持同步。

对于需要进行跨域访问的用户，跨域访问应遵循如下流程：

如果认证服务未从用户终端获取票据，认证服务需要对跨域用户认证，认证通过后为用户生成一个票据，调用票据存储接口将票据存储在用户本地并存储至国家中心 4A 系统的互信中心服务。

如果认证服务从用户终端读取票据，并调用票据验证接口到国家中心 4A 系统的互信中心服务验证票据是否有效，如果有效，用户不用认证继续访问。反之，用户需要在应用系统所在地的认证服务进行身份认证。具体接口详见附录 F。

6.3.1.2.3 授权管理

国家中心和各省中心的授权服务应严格遵循“谁的资源谁管理、谁的资源谁授权”的原则。对于跨区域访问的用户，由资源所在地的管理员根据用户所属中心、身份信息等为用户授予相应的权限。

6.3.1.2.4 审计管理

国家中心和各省中心的审计服务应严格遵循“谁的资源谁审计”的原则。对于跨域访问的用户，由资源所在地的审计服务对用户的所有访问进行审计。

6.3.2 各省与地市关系

各地市可以根据情况，选择建设 4A 系统或者使用各省中心建设的 4A 系统。具体的解

决方案可以参考附录 E。

7.应用安全平台建设规范

7.1 CA 系统建设规范

7.1.1 CA 系统功能建设规范

CA 系统主要是对生命周期内的数字证书全过程管理的安全系统。CA 系统主要是由证书签发系统、RA 系统、密钥管理系统和 LRA 等组成。CA 系统（SRRC-CA 中心）已由国家中心统一建设。

7.1.1.1 证书签发系统

证书签发系统提供了对生命周期内的数字证书进行全过程的管理的功能，包括证书/证书注销列表的生成与签发、证书/证书注销列表的存储与发布、证书状态的查询和密钥的生成与管理及安全管理等。

a) 证书/证书注销列表生成与签发系统

证书/证书注销列表生成与签发系统负责生成、签发数字证书和生成证书注销列表。签发的证书类型支持人员证书、设备证书和机构证书；并支持双证书机制（加密证书和签名证书）。

b) 证书状态查询系统

证书状态查询系统应为用户和应用系统提供证书状态查询服务，包括：

CRL 查询：用户或应用系统利用数字证书中标识的 CRL 地址，下载 CRL，并检验证书有效性；

在线证书状态查询：用户或应用系统按照 OCSP 协议，实时在线查询证书的状态。

c) 证书管理系统

证书管理系统是证书认证系统中实现对证书/证书注销列表的申请、审核、生成、签发、存储、发布、注销、归档等功能的管理控制系统。

d) 安全管理系统

安全管理系统主要包括安全审计系统和安全防护系统。

安全审计系统提供事件级审计功能，对涉及系统安全的行为、人员、时间等记录进行跟踪、统计和分析。

安全防护系统提供访问控制、入侵检测、漏洞扫描、病毒防治等网络安全功能。

7.1.1.2 RA 注册管理系统

用户注册管理系统负责用户的证书申请、身份审核和证书下载，可分为本地注册管理系统和远程注册管理系统。

国家中心应部署本地注册管理系统；各省分中心应部署远程注册管理系统。

a) 证书申请

证书申请可采用在线方式：各省中心用户通过专网登录到用户注册管理系统申请证书。

b) 身份审核

国家中心审核人员通过用户注册管理系统，对证书申请者进行身份审核。

c) 证书下载

证书下载可采用在线方式：各省中心用户通过专网等登录到用户注册管理系统下载证书。

7.1.1.3 密钥管理系统

密钥管理中心提供了对生命周期内的加密证书密钥对进行全过程管理的功能，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以及安全管理等。

a) 密钥生成

根据 CA 的请求为用户生成非对称密钥对，该密钥对由密钥管理中心的硬件加密设备生成。

b) 密钥存储

密钥管理中心生成的非对称密钥对，经硬件加密设备加密后存储在数据库中。

c) 密钥分发

密钥管理中心生成的非对称密钥对通过证书认证系统分发到用户证书载体中。

d) 密钥备份

密钥管理中心采用热备份、冷备份和异地备份等措施实现密钥备份。

e) 密钥更新

当证书到期或用户需要时，密钥管理中心根据 CA 请求为用户生成新的非对称密钥对。

f) 密钥撤销

当证书到期、用户需要或管理机构认为必要时，密钥管理中心根据 CA 请求撤销用户当前使用的密钥。

g) 密钥归档

密钥管理中心为到期或撤销的密钥提供安全长期的存储。

h) 密钥恢复

密钥管理中心可为用户提供密钥恢复服务和为司法取证提供密钥恢复服务。密钥恢复需按管理策略进行审批，一般用户只限于恢复自身密钥。

7.1.1.4 LRA 系统

LRA 系统为本地申请证书的用户信息进行注册。

7.1.2 性能指标

7.1.2.1 系统容量

CA 系统能支持 50000 个以上的用户证书的签发和管理。

7.1.2.2 响应速度

CA 系统数字证书的签发时间不超过 1 秒。

7.1.2.3 加密算法

CA 系统加密算法应符合国家相关法律和法规要求，并能对加密算法的种类和强度进行扩充和替换。

7.1.2.4 密钥保存期

密钥保存期不少于 10 年。

7.2 4A 系统建设规范

7.2.1 4A 系统功能建设规范

4A 系统主要为用户访问应用系统提供统一的身份管理、认证管理、授权管理、审计管理和组织机构管理等功能。主要是由身份管理、认证管理、授权管理、审计管理和组织机构管理等模块组成。4A 系统应遵循三员管理，4A 系统应能支持多种操作系统平台，并且对用户终端的操作系统无限制。

4A 系统与 SRRC-CA 中心的关系、国家中心 4A 系统与各省中心 4A 系统的关系及要求具体参见第 6 章。

7.2.1.1 身份管理

身份管理应支持从 SRRC-CA 中心同步用户信息，支持从智能密码钥匙 Key 证书导入用户信息，支持和第三方应用业务（数据库/LDAP）双向同步用户信息，支持以组织机构方式对用户进行分类管理，支持临时用户管理。

身份管理应能接管 BS 和 CS 应用系统账号信息，支持 Linux 主机、Windows 主机、数据库、LDAP、AD 域等多种账号同步方式，支持组、角色等多种账号授权方式。

用户信息库的存储建议采用 LDAP 方式，省级用户信息库与国家中心用户信息库的关系参见 6.3.1.2.1。应以 WebService 服务方式为应用系统提供组织机构及用户信息查询和读取接口，各省的应用系统如果需要读取组织机构及用户信息，直接从各省级用户信息库中读取，由各省自行定义。各省的组织机构信息和人员属性信息存储可参考附录 D 的 D.1 和 D.2。

7.2.1.2 身份认证

身份认证应能实现用户统一身份认证、单点登录功能；用户认证方式应能采用 SRRC-CA 中心发布的数字证书认证方式，应支持对网段、时间、IP 等多种认证策略设置。

应调用国家中心 4A 系统的互信中心服务提供的票据存储、读取和验证接口，实现 6.3.1.2.2 中所要求的跨域访问。具体接口详见附录 F。

7.2.1.3 授权管理

授权管理应支持入口级授权和细粒度授权；细粒度授权应支持资源的菜单级、URL 级的权限控制，应支持基于角色权限的配置管理；对于记录级、数据库字段级的授权可以由应用系统自行定义。

7.2.1.4 审计管理

审计管理应提供审计接口，支持其他应用系统的日志信息上报；支持用户行为关联审计；支持基于用户名、用户 IP、资源、时间的访问统计；支持日志的告警、自动清理管理等。

7.2.2 网络部署

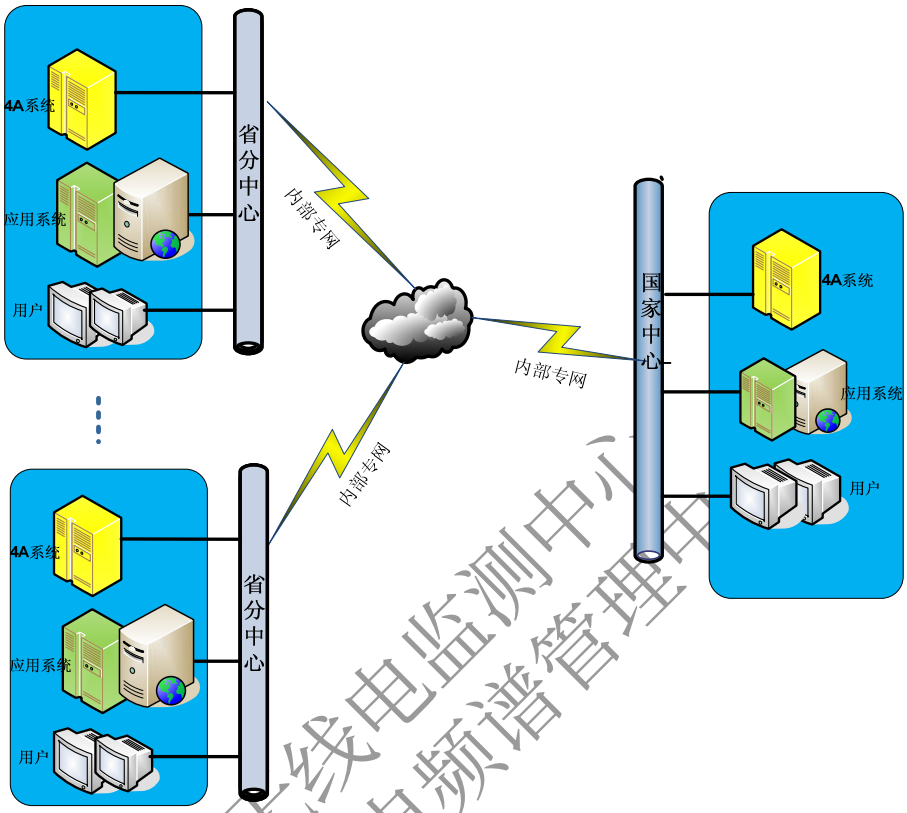

图2：4A系统部署图

国家中心和各省中心部署 4A 系统，为本中心用户和跨区域访问的用户提供身份管理、认证管理、授权管理和审计管理等服务。部署方式可以采用与应用系统并联、与应用系统串联等方式。

各地市可以根据情况，选择建设 4A 系统或者使用各省中心建设的 4A 系统。具体的解决方案可以参考附录 E。

7.2.3 性能建设规范

7.2.3.1 双机热备

应支持双机热备，支持主从设备之间的数据同步、故障切换和恢复回切。主从设备之间的切换时间小于 15 秒。

7.2.3.2 备份策略

4A 系统应能支持硬件、软件和数据库备份。

7.2.3.3 安全传输

用户终端与 4A 系统之间需建立起一个安全通道来保障数据传输的安全与完整。

7.2.3.4 运行稳定性

4A 系统应能保证系统提供 7×24 小时不间断服务。MTBF>100000 小时。

7.2.3.5 响应速度

4A 系统造成的系统延时不超过 1 秒。

8.应用系统安全规范

应用系统在实现应用安全平台提供的加解密、编码、数字签名、数字证书、安全协议、策略机制、审计服务、授权管理、访问控制、身份认证等服务的建设过程中，应用系统的开发和实施必须遵循如下规范。鉴于本次规范中只考虑 CA 系统提供的强身份认证功能，

8.1 基于 CA 系统建设规范

国家的 CA 认证中心颁发的数字证书完全符合 X.509 标准。应用系统要实现 CA 系统提供的身份认证、数据的完整性、机密性和不可抵赖性等功能，需要调用 CA 证书开发接口来完成服务，接口详见附录 G 的 CA 证书开发接口。

8.2 基于 4A 系统建设规范

a) 身份管理规范

已建设未被原有 AAA 系统接管和已被 AAA 系统接管的应用系统，4A 系统需要从应用系统上收集已有的用户账号，并进行账号映射授权，以实现单点登录功能。

新建的应用系统不需要新建账号，开发时依照 4A 系统提供的接口，直接调用 4A 系统提供的接口，接受 4A 系统推进的账号信息。

b) 认证管理规范

已建设未被原有 AAA 系统接管的和已被 AAA 系统接管的应用系统，应用厂商必须对应用系统进行改造，调用 4A 系统提供的接口，以实现用户认证和单点登录功能。

新建应用系统，开发时应依据 4A 系统提供的认证接口和单点登录接口，直接调用 4A 系统提供的接口来完成用户认证和单点登录功能。

c) 授权管理规范

已建设未被原有 AAA 系统接管的和已被 AAA 系统接管的应用系统如需实现统一授权，应用厂商必须对应用系统进行改造，调用 4A 系统提供的接口；

新建应用系统，开发时应依据 4A 系统提供的授权接口，接受 4A 系统推送过来的同名账号，基于同名账号进行统一授权。

d) 审计管理规范

已建设未被原有 AAA 系统接管的和已被 AAA 系统接管的应用系统如需实现统一审计，应用厂商必须对应用系统进行改造，调用 4A 系统提供的审计接口将审计信息。

新建应用系统，开发时应依据 4A 系统提供的审计接口，直接调用 4A 系统提供的接口来实现审计功能。

e) 组织机构管理规范

已建设未被原有 AAA 系统接管的和已被 AAA 系统接管的应用系统如需调用统一的组织机构及用户信息，应用厂商必须对应用系统进行改造，调用 4A 系统提供的组织机构查询和读取接口。新建应用系统，开发时应依据 4A 系统提供的组织结构查询和读取接口。

各省可以按照上述要求，在此基础上根据自身建设的 4A 系统出台相应的应用系统开发接口规范，并在规范中明确新建应用系统、已有应用系统的分别实现方式和接口服务等。国家中心应用系统的开发接口规范详见附录 H：《国家无线电监测中心 4A 系统接口规范》。

附录 A

证书申请使用管理规范

国家的 SRRC-CA 中心将按照有关程序，统一对全国无线电管理机构的工作人员、外单位的维护人员和各种安全实体对象（如 VPN 安全网关等）进行发证、认证。

a) 各地无线电管理机构用户证书及服务器证书应统一申请，经主管领导批准后发放，由专人操作，不得移交他人擅自操作，申请时需仔细核实用户有关信息，不得一人申请多证书或多人共用一个证书。

b) 各地无线电管理机构在申请证书时，在申请界面“是否备份加密密钥”处选中，用来备份数字证书。备份数据应由专人负责管理。

c) 用户数字证书有效期为 10 年。如需增加、变更或注销证书的，尽量安排在同一时间操作并电话或 E-MAIL 通知国家无线电监测中心相关负责人。

附录 B

区域代码表

国家中心区域代码为 0000，其他中心区域代码参照国家标准 GBT 2260-1999。

附录 C

证书读取接口

接口名称：getCACerts

接口描述：根据区域编码获取 CA 证书列表

传入参数：regionCode 字符串类型　区域代码

传出参数：Json 格式 CA 证书列表

[{username:00000001,regioncode:0000,cacert:<Base64的证书字符串信息1>},

{username:00000002,regioncode:0000,cacert:<Base64的证书字符串信息2>}]

附录 D

组织机构信息规范

D.1 存储结构

组织(o=organization)下的子树，就是按照“国家无线电管理机构”的实际组织机构结构进行分级存储，直观反映组织间的上下级关系。组织子树下包含属于该组织的人员列表，这里每个人只是一个索引，指向人员子树下具体的某个人员。

D.2 组织机构人员属性表

LDAP 字段	字段说明
cn	组织编码
displayName	组织名称
description	组织机构职能
custLevelid	组织架构层次
custParentOrgCode	上级组织编码
custParentOrgName	上级组织名称
member	组织成员（完整 dn）

D.3 组织机构信息同步规范

各省的用户身份信息、组织机构信息、用户身份与组织机构关系都基于模板，以 excel 格式提交至国家中心，由国家中心审核通过后，将该 excel 中的数据同步至国家中心用户信息库中。各省如果有用户信息修改，需要将修改信息提交至国家中心，各个模板如下：

D.4　用户身份信息模板

用户身份信息模板

填写规范：

1、粗体标*字段为必填项；

2、所有日期字段格式为：yyyy-mm-dd，例如：2013-09-17

3、性别可选值为：男/女；

4、任职状态可选值为：在职/离职；

5、直接上级主管允许有多个，填写上级主管用户名，以英文输入状态的逗号分隔。

***用户名**	***用户姓名**	***性别**	出生日期	***电子邮件**	办公电话	手机	通讯地址	***直接上级**	任职状态	入职时间	离职时间

D.5　组织机构信息模板

组织机构信息模板

填写规范：

1、粗体标*字段为必填项；

2、组织机构层级可选值为 0/10/20/30/40，国家无线电监测中心为 0，按行政组织机构递增；

3、上级组织机构名称为当前组织机构的上级组织机构全名；

4、组织机构成员可有多个，填写用户编码，以英文输入状态的逗号分隔。

***组织机构名称**	***组织机构职能描述**	***组织机构层级**	***上级组织机构名称**	组织机构成员
国家无线电监测中心	国家无线电监测中心为……	0		
信息管理处	……	10	国家无线电监测中心	00001201,00001202

注：列表原有数据为示例数据，实际填写时请将其清除。

D.6　提报信息模板

提报单位：	
提报时间：	
提报人：	
联系电话：	
提报信息说明：	

附录 E

地市应用安全平台建设方案

E.1 集中部署

地市需要使用省中心部署的 4A 系统来完成用户账号管理、认证、授权和审计等服务，如果地市有应用系统，也需要将地市的应用系统与 4A 系统做整合。网络部署结构如下：

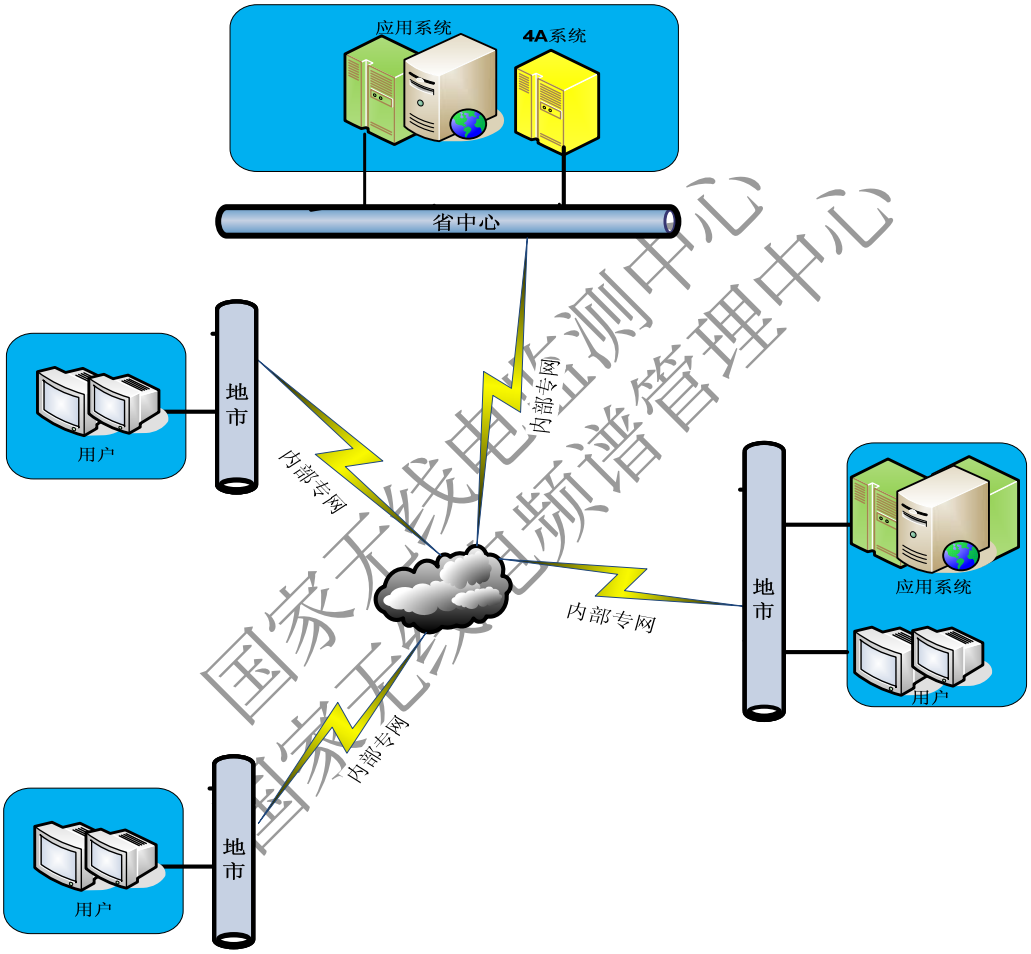

图 3：4A 系统集中部署图

E.2 应用场景

E.2.1 地市用户访问省中心的应用系统

a) 用户通过广域网首先登录省中心应用系统，应用系统发现用户没有合法的票据；

b) 应用系统将用户访问请求重定向到省中心的 4A 系统上；

c) 用户通过广域网在 4A 系统上进行认证，认证通过后，4A 系统返回用户票据；

d) 用户携带票据访问省中心应用系统，应用系统验证用户票据是否合法；如果票据合法，用户可以访问应用系统。

E.2.2 地市用户访问本地市应用系统

a) 用户通登录本地市的应用系统，应用系统发现用户没有合法的票据；

b) 应用系统将用户访问请求通过广域网重定向到省中心的 4A 系统上；

c) 用户通过广域网在4A系统上进行认证，认证通过后，4A系统通过广域网返回用户票据；

d) 用户携带票据访问应用系统，应用系统验证用户票据是否合法；如果票据合法，用户可以访问应用系统。

E.2.3 集中式部署特点

E.2.3.1 集中式部署优点

a) 节省费用，地市无需购买 4A 系统。

b) 方便省中心对地市的业务、人员的管控。

c) 地市级网络管理员维护简单。

E.2.3.2 集中式部署缺点

a) 地市用户访问容易受省中心和地市之间网络的影响，如果一旦网络有故障，地市用户就无法访问。

b) 访问速度慢。

c) 省级网络管理员维护工作量大。

E.2.4 分布式部署

地市可以建设 4A 系统来完成对本地市用户的账号管理、认证、授权和审计等服务。网络部署结构如下：

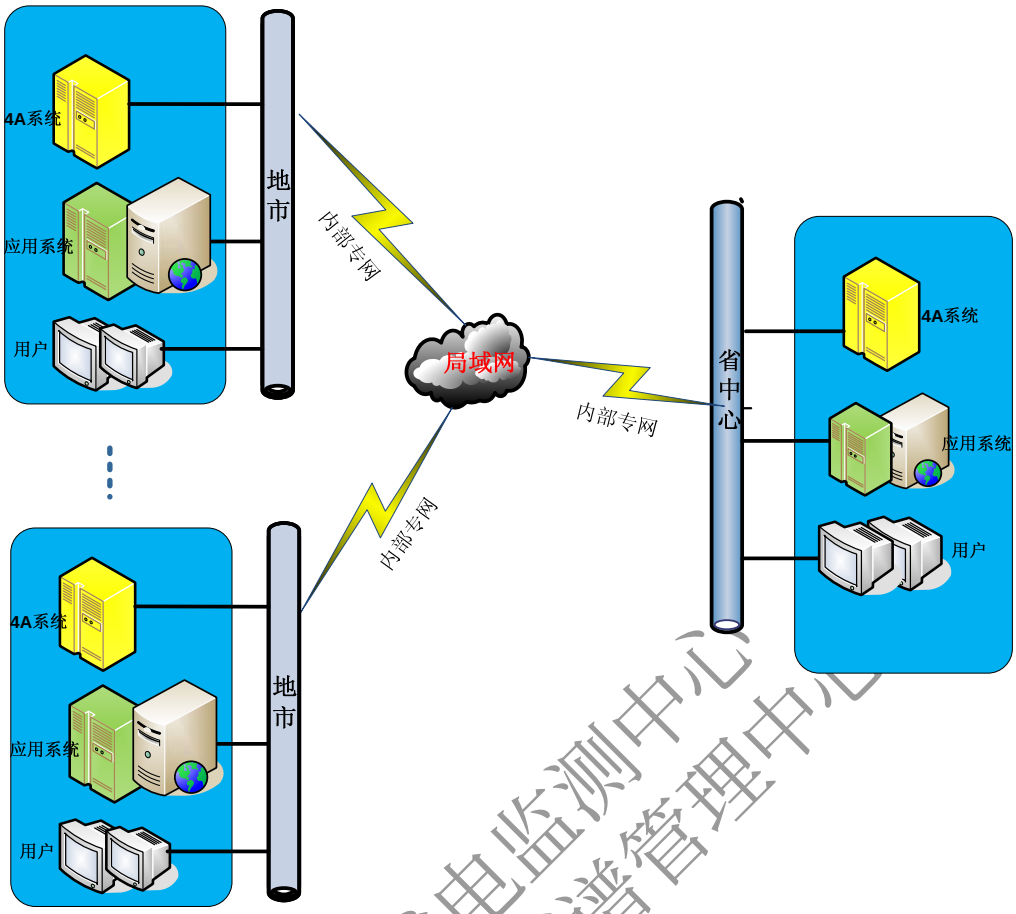

图 4: 4A 系统分布式部署图

E.3 应用场景

E.3.1 地市用户访问省中心的应用系统

a) 用户通过广域网首先登录省中心应用系统，应用系统发现用户没有合法的票据；

b) 应用系统将用户访问请求重定向到省中心的 4A 系统上；

c) 用户通过广域网在 4A 系统上进行认证，认证通过后，4A 系统返回用户票据；

d) 用户携带票据访问省中心应用系统，应用系统验证用户票据是否合法；如果票据合法，用户可以访问应用系统。

E.3.2 地市用户访问本地市应用系统

a) 用户通登录本地市的应用系统，应用系统发现用户没有合法的票据。

b) 应用系统将用户访问请求重定向到地市中心的 4A 系统上。

c) 用户在 4A 系统上进行认证，认证通过后，4A 系统返回用户票据。

d) 用户携带票据访问应用系统，应用系统验证用户票据是否合法；如果票据合法，用户可以访问应用系统。

E.3.3 分布式部署特点

E.3.3.1 分布式部署优点

a) 地市用户访问本地市的应用系统不受省中心和地市之间网络的影响。

b) 访问速度快。

E.3.3.2 集中式部署缺点

a) 花费较大，地市需要购买 4A 系统。

b) 不利用省中心对地市用户的管理控制。

c) 地市级维护困难维护相对困难，需要有专业的人员来维护。

附录 F

票据接口

F.1 票据存储

参数：认证票据

返回值：

a) 类型：String 类型

b) 格式：JSON 字符串格式

c) 实例：

1) 成功{“result”:”ok”}；

2) 失败{“result”:”error”,”errno”:”错误码”,”msg”:”错误消息”}

定义：String saveServiceTicket(String serviceTicket)

F.2 票据读取

参数：认证票据

返回值：成功，则返回认证票据

失败，则返回 NULL

定义：String getServiceTicket()；

F.3 票据验证

票据验证：

参数：认证票据

返回值：成功，则返回用户账号信息

失败，则抛出 InvalidTicketException

定义：String validateServiceTicket(String serviceTicket)；

附录 G

CA 证书开发接口

G.1 签名接口

功　能： key 内部私钥签名

参　数：[in]hCon　 容器句柄

[in]str 待签名的值

[in]strlen 待签名的长度

[out]signatrue 签名后的值

[out]signatruelen 签名后的值得长度

返回值： 成功，则返回 SCARD_SUCCESS（0）；

失败，则返回 SCARD_FAIL（1），或其它错误值。

定　义： DWORD InternalSignWithSM2Key (HANDLE hCon，

CHAR * str, INT * strlen, CHAR* signature,INT * signatureLen);

G.2 验签接口

功　能：key 内部公钥验签

参　数： [in]hCon　 容器句柄

[in]str 待签名的值

[in]strlen 待签名的长度

[in]signatrue 签名后的值

[in]signatruelen 签名后的值得长度

返回值： 成功，则返回 SCARD_SUCCESS（0）；

失败，则返回 SCARD_FAIL（1），或其它错误值。

定　义： DWORD InternalVerifyWithSM2Key (HANDLE hCon，

CHAR * str, INT * strlen, CHAR* signature, INT * signatureLen);

G.3 加密接口

功　能： key 内部公钥加密

参　数： [in]hCon 容器句柄

[in]str 待加密的值

[in]strlen 待加密值的长度

[in]encrypt 加密后的值

[in]encryptlen 加密后的值得长度

返回值： 成功，则返回 SCARD_SUCCESS（0）；

失败，则返回 SCARD_FAIL（1），或其它错误值。

定　义： DWORD InternalEncryptWithSM2Key (HANDLE hCon,

CHAR * str, INT * strlen, CHAR* encrypt, INT * encryptlen);

G.4 解密接口

功　能： key 内部解密

参　数： [in]hCon　容器句柄

[in]encrypt 加密值

[in]encryptlen 加密值的长度

[out]str 解密后的值

[out]strlen 解密后值的长度

返回值： 成功，则返回 SCARD_SUCCESS（0）；

失败，则返回 SCARD_FAIL（1），或其它错误值。

定　义： DWORD InternalDecryptWithSM2Key (HANDLE hCon,

CHAR* encrypt, INT * encryptlen, CHAR * str, INT * strlen);

附录 H

接口规范

《国家无线电监测中心 4A 系统接口规范》。