ICS 13.310
A 91

GA

中华人民共和国公共安全行业标准

GA/T 669.2—2008

城市监控报警联网系统　技术标准
第2部分：安全技术要求

Technical standard of city area monitoring and alarming network system—Part 2：Technical specification of security

2008-08-04 发布　　2008-08-04 实施

中华人民共和国公安部　发布

目　次

前　言

请注意，本部分的基本内容有可能涉及专利，本部分的发布机构不应承担识别这些专利的责任。

GA/T 669《城市监控报警联网系统　技术标准》分为11个部分：

——第1部分：通用技术要求；

——第2部分：安全技术要求；

——第3部分：前端信息采集技术要求；

——第4部分：视音频编、解码技术要求；

——第5部分：信息传输、交换、控制技术要求；

——第6部分：视音频显示、存储、播放技术要求；

——第7部分：管理平台技术要求；

——第8部分：传输平台技术要求；

——第9部分：卡口信息识别、比对、监测系统技术要求；

——第10部分：无线视音频监控系统技术要求；

——第11部分：关键设备通用技术要求。

本部分为GA/T 669的第2部分。

本部分的附录A、附录B为规范性附录，附录C为资料性附录。

本部分由公安部科技局提出。

本部分由全国安全防范报警系统标准化技术委员会(SAC/TC 100)归口。

本部分起草单位：公安部第一研究所、北京中盾安全技术开发公司、北京网新中广科技发展有限责任公司、杭州恒生数字设备科技有限公司、武汉大学国家多媒体工程中心、深圳中兴力维技术有限公司、杭州华三通信技术有限公司、杭州思福迪信息技术有限公司、北京联视神盾安防技术有限公司。

本部分主要起草人：房子河、栗红梅、陈朝武、张俊业、王楠、张本锋、崔云红、赵惠芳、刘剑、胡瑞敏、查敏中、王学华、戚文雅、向稳新、张鹏国、王海增、李晓峰、杨国胜、陆品祥、王娜。

城市监控报警联网系统　技术标准
第2部分:安全技术要求

1　范围

GA/T 669的本部分规定了城市监控报警联网系统(简称联网系统)安全设计原则、安全技术体系总体框架和认证及权限管理结构、物理安全、通信和网络安全、运行安全、信息安全等基本技术要求,是进行城市监控报警联网系统安全建设规划、方案设计、工程实施、系统检测验收以及与之相关的系统设备研发、生产的依据。

本部分适用于城市监控报警联网系统,其他领域的监控报警联网系统可参考采用。

2　规范性引用文件

下列文件中的条款通过GA/T 669的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 2260—2007　中华人民共和国行政区划代码

GB/T 2659—2000　世界各国和地区名称代码(eqv ISO 3166-1:1997)

GB 4943—2001　信息技术设备的安全(idt IEC 60950:1999)

GB/T 7408—2005　数据元和交换格式　信息交换　日期和时间表示法(ISO 8601:2000,IDT)

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

GB 50348—2004　安全防范工程技术规范

GA/T 367—2001　视频安防监控系统技术要求

GA/T 669.1—2008　城市监控报警联网系统　技术标准　第1部分:通用技术要求

GA/T 669.5—2008　城市监控报警联网系统　技术标准　第5部分:信息传输、交换、控制技术要求

GA/T 669.7—2008　城市监控报警联网系统　技术标准　第7部分:管理平台技术要求

RFC 3280　X.509公钥证书和CRL

3　术语、定义和缩略语

GA/T 669.1—2008中确立的以及下列术语、定义和缩略语适用于本部分。

3.1　术语和定义

3.1.1

公钥基础设施　public key infrastructure

包括硬件、软件、人员、策略和规程的集合,用来实现基于公钥密码体制证书的产生、管理、存储、分发和撤销等功能。

3.1.2

公钥证书　public key certificate

用户的公钥连同其他信息,并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

3.1.3

证书认证机构　certification authority

负责创建和分配证书,受用户信任的权威机构。用户可以选择该机构为其创建密钥。

3.1.4

注册机构　registration authority

为用户办理证书申请、身份审核、证书下载、证书更新、证书注销以及密钥恢复等实际业务的办事机构或业务受理点。

3.1.5

证书撤销列表　certificate revocation list

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除了普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

3.1.6

权限管理系统　privilege management system

为用户、角色分配权限，并保障其正确使用的系统。

3.1.7

安全管理系统　security management system

负责对用户信息及安全事件进行管理并完成安全审计等功能的系统。

3.1.8

安全支撑平台　security supporting platform

完成用户身份认证及单点登录、设备接入认证、数字签名、数据加密和访问控制等功能的系统。

3.1.9

物理安全　physical security

联网系统设备所处的物理环境的安全，是整个系统安全运行的前提。

3.1.10

运行安全　operation security

网络与信息系统的运行过程和运行状态的安全。

3.1.11

信息安全　information security

信息在数据收集、存储、检索、传输、交换、显示、扩散等过程中的安全，使得在数据处理层面保障信息依据授权使用，保护信息不被非法冒充、窃取、篡改、抵赖。

3.1.12

安全子系统　security subsystem

联网系统的一部分，包括公钥基础设施、权限管理系统、安全管理系统及安全支撑平台软硬件。

3.1.13

安全域　security domain

计算机网络中从属于单一安全策略、受单个授权机构管理的多个实体构成的集合。

3.2　缩略语

AES　Advanced Encryption Standard　高级加密标准

CRL　Certificate Revocation List　证书撤销列表

DES　Data Encryption Standard　数据加密标准

MD5　Message Digest Algorithm 5　信息摘要 5

NTP　Network Timing Protocol　网络时间协议

PKI/CA　Public Key Infrastructure/Certification Authority　公钥基础设施/认证机构

PMS	Privilege Management System　权限管理系统
SHA	Secure Hash Algorithm　安全哈希算法
SNTP	Simple Network Time Protocol　简单网络时间协议
SSL	Secure Socket Layer　安全套接字
S/MIME	Secure/Multipurpose Internet Mail Extensions　安全多用途网际邮件扩充协议
TSA	Time Stamp Authority　时间戳机构
TLS	Transport Layer Security　传输层安全
URL	Uniform Resource Locator　统一资源定位符
VPN	Virtual Private Network　虚拟专用网络

4　联网系统安全设计原则

4.1　规范性原则

联网系统安全设计应符合国家或行业相应的安全标准。

4.2　先进性和实用性原则

联网系统安全设计应采用先进的设计思想和方法，尽量采用国内、外先进技术（例如：主动防御技术等）。所采用的先进技术应符合当地环境条件、监视对象、监控方式、维护保养以及投资规模等实际情况；应合理设置系统功能、恰当进行系统配置和设备选型，保证其具有较高的性价比，满足业务管理的需求。

4.3　可扩展性原则

联网系统安全设计应考虑通用性、灵活性，以便利用现有资源及应用升级。

4.4　开放性和兼容性原则

对安全子系统的升级、扩充、更新以及功能变化应有较强的适应能力。即当这些因素发生变化时，安全子系统可以不作修改或作少量修改就能在新环境下运行。

4.5　可靠性原则

联网系统安全设计应确保系统的正常运行和数据传输的正确性，在硬件的选型和配置、软件的组织和设计方法的选择、数据的安全性和完整性以及系统的运行和管理等方面都应采取必要的措施。防止由内在因素和硬件环境造成的错误和灾难性故障，确保系统可靠性。

4.6　系统性原则

应采用系统优化设计，综合考虑安全子系统的整体性、相关性、目的性、实用性和环境适应性。另外，与应用系统的结合应相对简单、独立。

4.7　技术与管理相结合原则

联网系统安全体系应遵循技术与管理相结合的原则进行设计和实施，各种安全技术应该与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合，从社会系统工程的角度综合考虑，最大限度发挥人防、物防、技防相结合的作用。

4.8　等级保护原则

应根据应用需求确定信息安全等级保护级别，并遵照信息安全等级保护原则，选择适合系统的安全保护措施。

4.9　分层安全原则

按照设备的使用范围以及层次性、多监控中心的结构，设计相应的安全域，安全域内应进行安全认证和权限分配，保证相关业务和影响仅在有限范围内进行，控制权限的蔓延。

4.10　最小权限原则

为设备或用户分配权限时，应在不影响业务的情况下，实现功能明确、设备明确、时段明确和“权限最小化”，以有效进行权限管理。

5 联网系统安全技术体系总体框架和认证及权限管理结构

5.1 总体框架

联网系统安全技术体系总体框架如图1所示，可以分为物理(实体)安全、通信和网络安全、运行安全以及信息(数据)安全四个层面。

物理安全主要包括监控中心电源安全、电磁兼容性安全、环境安全、设备安全、防雷接地、记录介质安全六个方面。

通信和网络安全主要包括网络传输安全、公安专网的接入安全、公安专网的输出安全三个方面。

运行安全主要包括安全监控、安全审计、恶意代码防护、备份与故障恢复、应急处理、安全管理六个方面。

信息安全主要包括用户身份认证、接入设备认证、用户权限管理、访问控制及业务审计、数据加密及数据完整性保护、安全域隔离六个方面。

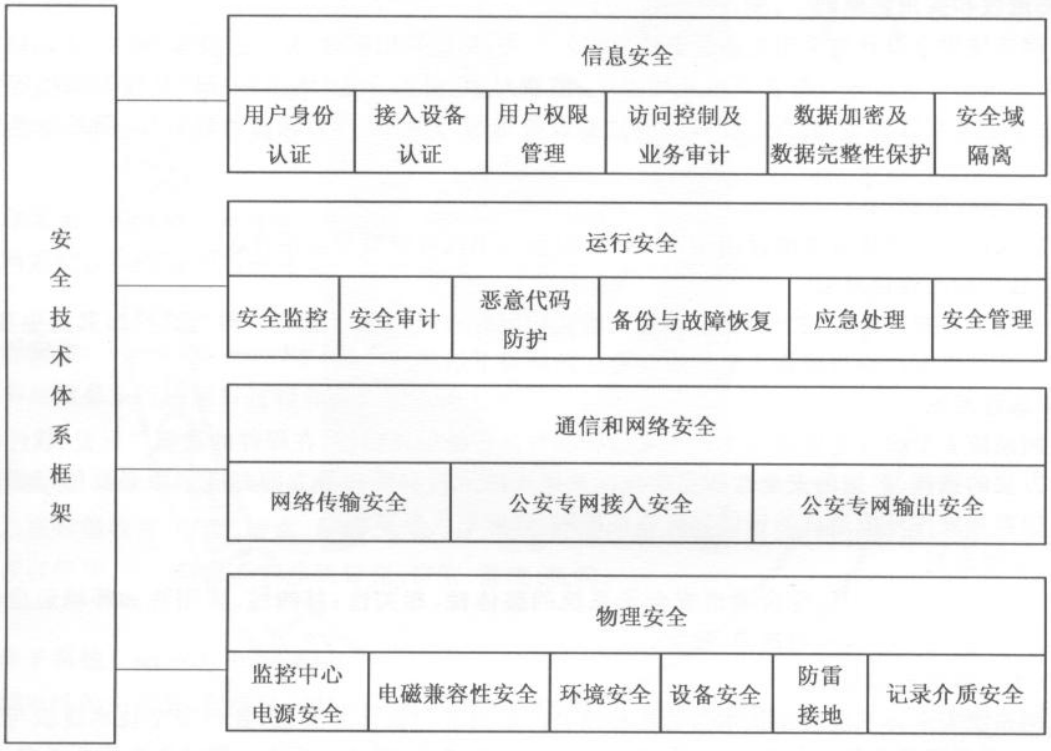

图1 安全技术体系总体框架

5.2 认证及权限管理结构

联网系统认证及权限管理结构如图2所示。公钥基础设施(PKI)和权限管理系统(PMS)都通过安全管理系统为安全支撑平台提供基础服务。公钥基础设施(PKI)为联网系统设备和用户发放数字证书，并提供对证书有效性以及证书撤销列表(CRL)的查询服务。权限管理系统(PMS)保存系统权限策略和权限数据，为用户提供权限查询服务。安全管理系统负责用户管理，并从公钥基础设施(PKI)获取数字证书和CRL信息，从权限管理系统(PMS)获取权限信息，为安全支撑平台提供基础服务。

安全支撑平台为联网系统提供用户身份认证及单点登录、接入设备认证、数字签名、数据加密、访问控制等安全服务，以保证应用系统的可用性、完整性和机密性。

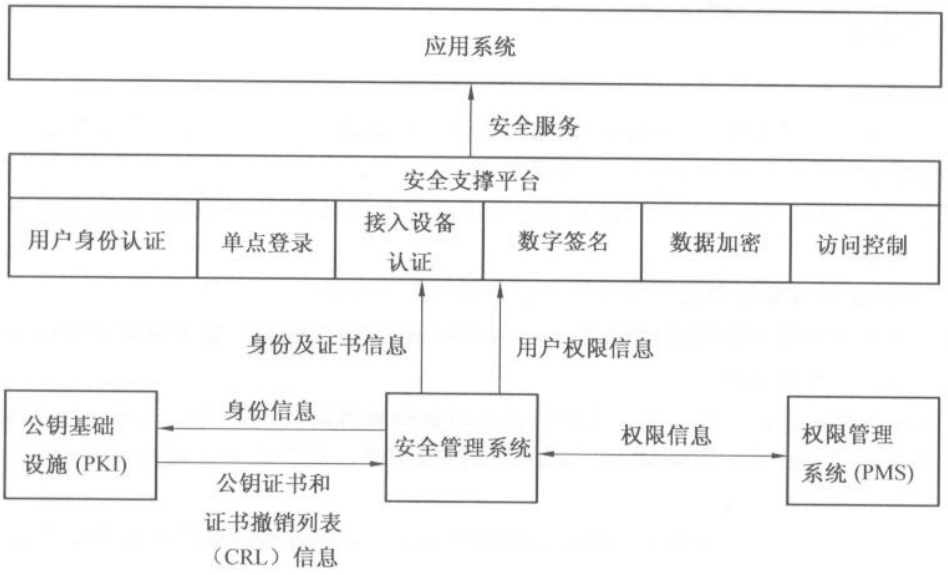

图 2　认证及权限管理结构

6　物理安全

6.1　监控中心电源安全

监控中心配电系统应满足 GB 50348—2004 中 3.12 的要求。

监控中心应配备用电源，备用电源应能保证对监控中心内关键设备延长供电不少于 8 h。

6.2　电磁兼容性安全

联网系统抗电磁干扰性能应满足 GA/T 367—2001 中 9.1 的要求；传输线路的抗干扰设计应符合 GB 50348—2004 中 3.6.2 的规定。

联网系统电磁辐射防护性能应满足 GA/T 367—2001 中 9.2 的要求。

6.3　环境安全

监控中心机房应满足 GB/T 20271—2006 中 4.1.1.1 的要求，选择机房场地、实现机房内部安全防护、防火、防水、防潮、空调降温、防静电。

通信线路的安全应按照 GB/T 20271—2006 中 4.1.1.2 的要求对通信线路进行安全防护。

6.4　设备安全

主要指三类设备：联网系统前端设备、通讯设备（路由器、交换机等）和监控中心主机设备（终端计算机、服务器等）。根据设备所处位置的不同，又可分为室内设备、室外设备和移动设备。

应按照 GB/T 20271—2006 中 4.1.2.1 的设备标记要求、计算中心防盗要求和机房外部设备防盗要求，实现设备的安全保护。

应按照 GB/T 20271—2006 中 4.1.2.2 的基本运行支持要求、安全可用要求和不间断运行要求设计和实现设备的可用程度。

硬件设备应符合 GB 4943—2001 中关于电击、火灾、发热、机械、辐射、化学等安全方面的要求。

6.5　防雷接地

应综合设计系统的防雷和接地。系统各组成部分的防雷和接地设计应符合 GB 50348—2004 中 3.9的规定。

6.6　记录介质安全

应按照 GB/T 20271—2006 中 4.1.3 的公开数据介质保护、内部数据介质保护、重要数据介质保护、关键数据介质保护和核心数据介质保护的要求进行记录介质安全保护。

7 通信和网络安全

7.1 网络传输的安全

当联网系统使用公安专网、公共网络、无线网络进行传输时，应分别符合相关部门对各个网络的安全管理规定或标准。

公共网络、无线网络在条件允许的情况下宜采用虚拟专用网络(VPN)或者传输层安全(TLS)协议来保证传输的安全。

7.2 公安专网的接入与输出安全

公安专网应专网专用，当其他网络需要与公安专网进行数据交换时，应采取相应措施保障公安专网的安全。宜在如下方案中选择：

a) 将模拟视频输出信号接入由公安部门认可的视频编码设备，然后接入公安监控系统。

b) 社会监控中心将数字图像单向传输给公安监控中心。当与公安专网接口时，应符合公安专网的安全管理规定。

c) 公安监控中心将数字图像输出给社会监控中心时，应按照公安专网的安全管理规定经安全隔离设备后方可输出。

7.3 双网并存

当不能解决公安专网与其他网络的隔离问题时，宜在公安监控中心设置两套完全物理隔离的监控系统，一套直接连接公安专网，另一套连接社会监控中心。

8 运行安全

8.1 安全监控

应按照 GB/T 20271—2006 中 4.2.3 的要求，设置分布式探测器，实时监测网络数据流，监视和记录内、外部用户出入网络的相关操作。宜使用防火墙、防毒软件、入侵检测系统、漏洞扫描工具来提高网络通信的安全性。

8.2 安全审计

应按照 GB/T 20271—2006 中 4.2.4 的要求，支持对审计功能的开启和关闭，对身份鉴别、管理用户/业务用户所实施的操作、其他与系统安全相关的事件等实施审计，并做出相应的审计响应。

安全审计日志宜采用统一的格式，数据项应包括：

a) 操作人身份：用户身份标识；

b) 操作：功能操作；

c) 操作对象：操作的对象(如 DVR 设备)；

d) 操作类型：日志管理，用户管理，配置管理，任务管理等；

e) 操作时间：年、月、日、时、分、秒；

f) 操作结果：成功、失败。

安全审计的日志记录信息应能够提供导入、导出、查询等功能。

8.3 恶意代码防护

应按照 GB/T 20271—2006 中 4.2.7 的要求，对包括计算机病毒在内的恶意代码进行有效的安全防护。

8.4 备份与故障恢复

8.4.1 联网系统应对系统的基本配置信息、用户信息、设备信息、权限信息、报警信息、巡检信息、与报警关联的视音频信息、重要事件的视频图像、系统重要操作日志等进行分类并做相应的定期备份。

8.4.2 关键存储部件宜采用冗余磁盘阵列技术并支持失效部件的在线更换；对重要的设备应进行冗余配置，以实现双机热备或者冷备。

8.4.3 数据库服务器宜采用双机冗余热备份的方式。进行定期在线维护，以实现当数据库遭到破坏时，缩短恢复所需时间。

8.4.4 在条件具备的情况下，应在异地建立和维护一个重要数据的备份存储系统，利用地理上的分离来保证系统和数据对灾难性事件的抵御能力。

8.4.5 故障恢复前应制定具体合理的恢复工作计划，故障恢复方案应根据信息备份方案制定，数据恢复完成后应检测数据的完整性。

8.5 应急处理

应制定安全应急处理预案，并组织实施应急处置演习。对系统在正常工作中发生的突发事件(各类异常情况、安全事件、安全事故)，应由值班人员或者维护人员依照应急处理预案进行处置或系统自动降级处理。

8.6 安全管理

各级各类监控中心应建立完善的安全管理制度，对监控中心的工作人员应进行安全管理教育和定期技术培训。

应对组成系统的各种设备定期进行安全检查和维护。

9 信息安全

9.1 公钥基础设施

9.1.1 证书认证机构(CA)

联网系统应建立CA机构。其主要职责如下：

a) 为本辖区内用户、设备签发证书；

b) 本级证书撤销列表(CRL)的创建和维护；

c) 管理、维护所签发的证书。

9.1.2 数字证书类型

联网系统PKI体系涉及三种证书类型：

a) 用户证书；

b) 设备证书，其中包括服务器证书和其他设备证书；

c) CA证书。

用户是指公安用户及政府其他部门需要共享监控业务信息的用户；设备是指服务器和其他设备；CA证书是指认证机构自身的证书。

9.1.3 证书格式

应支持X.509 V3标准证书，并支持所有X.509 V3标准定义的扩展。应支持X.509 V2证书撤销列表(CRL)。统一的用户证书格式、设备证书格式见附录A.1和A.2；统一的CRL格式见附录B。

9.1.4 证书载体

联网系统所签发的证书应支持以下方式存储：

a) 移动存储介质：如硬盘、U盘、存储IC卡等；

b) 硬盘：通过文件的方式存储在硬盘上或通过证书管理器进行存储和管理；

c) 智能卡：带有算法的IC卡；

d) USBKey：USB接口的、带有算法的令牌；

e) 专用加密设备：如加密机，通常用于产生、存储和管理密钥和公钥证书。

9.2 系统时间校正

联网系统应采用网络时间协议(NTP)来实现系统的时间校正。在时间精度要求不高的情况下宜以系统中的一台主服务器时间为基准实现全网时间校正；当时间精度要求较高时宜采用GPS授时技术获取标准时间，采用简单网络时间协议(SNTP)来实现系统时间校正。当时间戳做为可信依据时宜引

入时间戳机构(TSA),采用直接连接时间传输技术提供可信赖的且不可抵赖的时间戳服务。时间校正周期可根据实际情况设定。

9.3 用户身份认证

9.3.1 用户身份标识

应对联网系统的所有用户进行统一的唯一标识,编码规范见 GA/T 669.7—2008 中第 9 章的要求。

9.3.2 用户身份认证机制

联网系统应在以下方式中选择一种或者多种方式进行用户身份认证。

a) 静态口令机制(用户名/密码方式);

b) 动态口令机制;

c) 基于智能卡的认证;

d) 基于冲击/响应的 USBKey 认证;

e) 基于 PKI/CA 体系数字证书的 USBKey 认证;

f) 基于人体生物特征识别的认证。

采用基于 PKI/CA 体系数字证书的 USBKey 认证方式时应采用统一的公钥证书格式。对系统管理员、超级管理员宜附加基于人体生物特征识别的认证。

基于数字证书和静态口令两种方式的用户身份认证过程参见附录 C。

9.3.3 单点登录与全网漫游

联网系统应支持授权用户单点登录与全网漫游的功能。

9.3.3.1 单点登录功能要求:

a) 联网系统应支持用户只经过一次身份认证,即可访问不同安全域的应用系统。

b) 联网系统 Web 服务器、应用服务器应在用户身份认证成功后,保存用户的认证标识和身份标识。当用户访问不同的安全域时,Web 服务器、应用服务器后台应用程序应根据其身份标识来确定该用户的用户类型。

9.3.3.2 全网漫游功能要求:

a) 联网系统应采用统一的公钥证书格式,以保证在各级应用系统中均可被识别;

b) 联网系统应采用统一的认证方式,以保证不同安全域之间用户的身份认证。

9.4 接入设备认证

9.4.1 应对接入联网系统的所有设备进行统一的唯一标识,编码规范见 GA/T 669.7—2008 中第 9 章的要求。

9.4.2 接入设备认证应根据不同情况采用不同的认证方式。对非 SIP 设备,宜通过设备代理来进行认证;对标准 SIP 可信设备应采用数字证书的认证方式。设备认证的流程见 GA/T 669.5—2008 中第 8 章、第 9 章的要求。

9.5 用户授权策略与权限管理

9.5.1 用户分类

根据用户对联网系统使用性质的不同,将用户分为两大类:

a) 业务用户:使用系统执行业务操作的用户(例如访问实时视频、访问历史业务信息、进行摄像机云台、镜头控制等操作)。

b) 管理用户:能够对系统软硬件资源、系统运行状态以及安全配置等进行管理的用户。

联网系统宜根据实际需求按照用户职责细化用户分类。业务用户通常可细化为操作员、值班员等;管理用户通常可细化为系统管理员、安全管理员等。

用户宜赋予不同的优先级。

联网系统宜按照一定的规则将具有相同属性或特征的用户划分为一组,进行用户组管理。

9.5.2 授权策略

授权应遵循以下策略：

a) 联网系统应制定符合实际情况的授权模型；

b) 基础授权策略标准应统一；

c) 各级监控中心各自对用户授权。

9.5.3 权限管理

用户权限分为两大类：业务权限和管理权限。业务用户不应具备管理权限。

在监控中心内，权限管理应包括下列内容：

a) 提供增加、修改、删除和查询用户权限等功能。

b) 单独设立安全管理员，专门负责为本中心的每个合法用户分配相应的权限。除安全管理员外，任何用户不得擅自更改其权限、不得越权操作、不得将其权限转授给其他用户。安全管理员除完成授权功能外，不能浏览、修改、删除系统中的任何其他数据。

c) 高优先级用户可抢占低优先级用户所占用的资源。

在监控中心间，用户权限管理应在各级监控中心授权的基础上进行。

9.6 访问控制与业务审计

9.6.1 访问控制

联网系统应实现统一的用户管理和授权，在身份鉴别的基础上，系统宜采用某种访问控制模型对用户进行访问控制(例如基于角色的访问控制或者基于属性证书的访问控制)。基于角色的访问控制应提供对委托授权和角色继承功能的支持；角色管理应能提供角色的增加、修改、删除等功能，并且对角色的操作提供审计接口。

9.6.2 业务审计

联网系统应对以下事件进行业务审计，并保留记录，以备查验。

a) 用户登录和身份验证；

b) 非法或异常事件；

c) 用户越权行为；

d) 持有权限变更操作。

9.7 数据加密及数据完整性保护

9.7.1 联网系统应对需要加密的数据在传输和存储过程中进行加密，存储时宜采用 3DES、密钥长度为 128 位的高级加密标准(AES)、SCB2 算法等进行加密；传输过程中宜采用 RSA(1 024 位或 2 048 位)对会话密钥进行加密，传输内容宜采用数据加密标准(DES)、3DES、AES(128 位) 等算法加密。

9.7.2 对信令数据的加密宜采用 SIP 协议所支持的安全多用途网际邮件扩充协议(S/MIME)进行处理。

9.7.3 联网系统宜采用数字摘要、数字时间戳及数字水印等技术防止信息的完整性被破坏，即防止恶意篡改系统数据。数字摘要宜采用信息摘要 5(MD5)、安全哈希算法 1(SHA-1)、安全哈希算法 256(SHA256)等算法。

9.8 安全域隔离

应将联网系统划分为不同的安全域，如监控中心局域网、公安专网、公共网络等，不同的安全域之间应进行相应的隔离。当需要在公网和专网之间进行数据交换时，应采用国家、行业管理部门认可的安全隔离措施。

附 录 A
（规范性附录）
支持 X.509 V3 的证书格式定义

A.1 用户证书格式

用户证书格式见表 A.1。

表 A.1 用户证书格式定义

序号	数据项名称		数据类型	数据长度	采用标准	说 明
1	版本号		整型	1 字节	RFC 3280	证书格式版本号，目前为 3
2	序列号		字符型	32 字节	RFC 3280	证书序列号，用于证书管理，每一 CA 系统中，应为唯一值
3	签名算法		字符型	16 字节	RFC 3280	CA 中心签名该证书使用的算法
4	签发单位	名称(CN)	字符型	8 字节		签发该证书的 CA 中心的信息
		区/县(L)	字符型	2 字节	GB/T 2260—2007	
		地市(L)	字符型	2 字节	GB/T 2260—2007	
		省份(S)	字符型	2 字节	GB/T 2260—2007	
		国家(C)	字符型	2 字节	GB/T 2659—2000	
5	有效期	生效日期	字符型	19 字节	GB/T 7408—2005	证书生效日期，格式例如：2007-08-12 12:23:34
		失效日期	字符型	19 字节	GB/T 7408—2005	证书失效日期，格式例如：2007-08-18 12:23:34
6	证书持有者信息	用户名称(CN)	字符型	48 字节		姓名 身份证号码
		区/县(L)	字符型	2 字节	GB/T 2260—2007	
		地市(L)	字符型	2 字节	GB/T 2260—2007	
		省份(S)	字符型	2 字节	GB/T 2260—2007	
		国家(C)	字符型	2 字节	GB/T 2659—2000	
7	证书持有者公钥信息		字符型	1 024 位	RFC 3280	持证人的公开密钥信息
8	扩展项	CRL 分布点	字符型	128 字节	RFC 3280	
		证书持有者密钥标识符	字符型	20 字节	RFC 3280	
		签发单位的密钥标识符	字符型	20 字节	RFC 3280	
		密钥用途	字符型	64 字节	RFC 3280	
		预留	字符型	128 字节		待以后扩充
9	签名项		字符型	1 024 位	RFC 3280	CA 中心对该证书的签名

A.2 设备证书格式

设备证书格式见表 A.2。

表 A.2 设备证书格式定义

序号	数据项名称		数据类型	数据长度	采用标准	说　明
1	版本号		整型	1 字节	RFC 3280	证书格式版本号，目前为 3
2	序列号		字符型	32 字节	RFC 3280	证书序列号，用于证书管理，每一 CA 系统中，应为唯一值
3	签名算法		字符型	16 字节	RFC 3280	CA 中心签名该证书使用的算法
4	签发单位	名称(CN)	字符型	8 字节		签发该证书的 CA 中心的信息
		区/县(L)	字符型	2 字节	GB/T 2260—2007	
		地市(L)	字符型	2 字节	GB/T 2260—2007	
		省份(S)	字符型	2 字节	GB/T 2260—2007	
		国家(C)	字符型	2 字节	GB/T 2659—2000	
5	有效期	生效日期	字符型	19 字节	GB/T 7408—2005	证书生效日期，格式例如：2007-08-12 12:23:34
		失效日期	字符型	19 字节	GB/T 7408—2005	证书失效日期，格式例如：2007-08-18 12:23:34
6	证书持有者信息	设备名称(CN)	字符型	48 字节		
		区/县(L)	字符型	2 字节	GB/T 2260—2007	
		地市(L)	字符型	2 字节	GB/T 2260—2007	
		省份(S)	字符型	2 字节	GB/T 2260—2007	
		国家(C)	字符型	2 字节	GB/T 2659—2000	
7	证书持有者公钥信息		字符型	1 024 位	RFC 3280	持证人的公开密钥信息
8	扩展项	CRL 分布点	字符型	128 字节	RFC 3280	
		证书持有者密钥标识符	字符型	20 字节	RFC 3280	
		签发单位的密钥标识符	字符型	20 字节	RFC 3280	
		密钥用途	字符型	64 字节	RFC 3280	
		预留	字符型	128 字节		以后扩充
9	签名项		字符型	1 024 位	RFC 3280	CA 中心对该证书的签名

附 录 B
（规范性附录）
支持 X.509 V2 的证书撤销列表(CRL)格式

B.1 X.509 V2 证书撤销列表 CRL 格式

X.509 V2 证书撤销列表 CRL 格式见表 B.1。

表 B.1 X.509 V2 证书撤销列表 CRL 格式

序号	数据项名称		数据类型	数据长度	采用标准	说 明
1	版本号		整型	1 字节	RFC 3280	CRL 的版本号
2	签发单位	名称(CN)	字符型	8 字节		CRL 签发者的信息，CRL 的签发者为签发该类公钥证书的相应 CA 中心
		区/县(L)	字符型	2 字节	GB/T 2260—2007	
		地市(L)	字符型	2 字节	GB/T 2260—2007	
		省份(S)	字符型	2 字节	GB/T 2260—2007	
		国家(C)	字符型	2 字节	GB/T 2659—2000	
3	发布时间	生效时间	字符型	19 字节	GB/T 7408—2005	该 CRL 发布的时间，格式例如：2007-08-12 12:23:34
		下次更新的时间	字符型	19 字节	GB/T 7408—2005	下一 CRL 发布时间，格式例如：2007-08-18 12:23:34
4	签名算法		字符型	16 字节	RFC 3280	CA 中心签名该 CRL 使用的算法
5	扩展项	签发单位的密钥标识符	字符型	20 字节	RFC 3280	签发单位的密钥标识符
		CRL 分布点	字符型	128 字节	RFC 3280	CRL 分布点
6	吊销列表（包括吊销证书 1～N 个）	撤销证书的序列号	字符型	32 字节	RFC 3280	
		证书吊销日期	字符型	19 字节	GB/T 7408—2005	该证书被吊销的时间，格式例如：2007-08-12 12:23:34
		证书注销原因	整型	1 字节	RFC 3280	证书注销原因见表 B.2
7	签名项		字符型	1 024 位	RFC 3280	CA 中心对该 CRL 的签名

B.2 X.509 V2 证书撤销列表 CRL 格式的证书注销原因编码

X.509 V2 证书撤销列表 CRL 格式中证书注销原因编码见表 B.2。

表 B.2 证书注销原因编码表

证书注销原因名称	证书注销原因编码
未指明原因	0
密钥泄密	1
CA 泄密	2
从属关系改变	3
证书被取代	4
操作终止	5
证书冻结	6

附 录 C
（资料性附录）
数字证书和静态口令两种方式下的用户身份认证流程

C.1 用户身份认证流程图

用户身份认证流程见图 C.1：

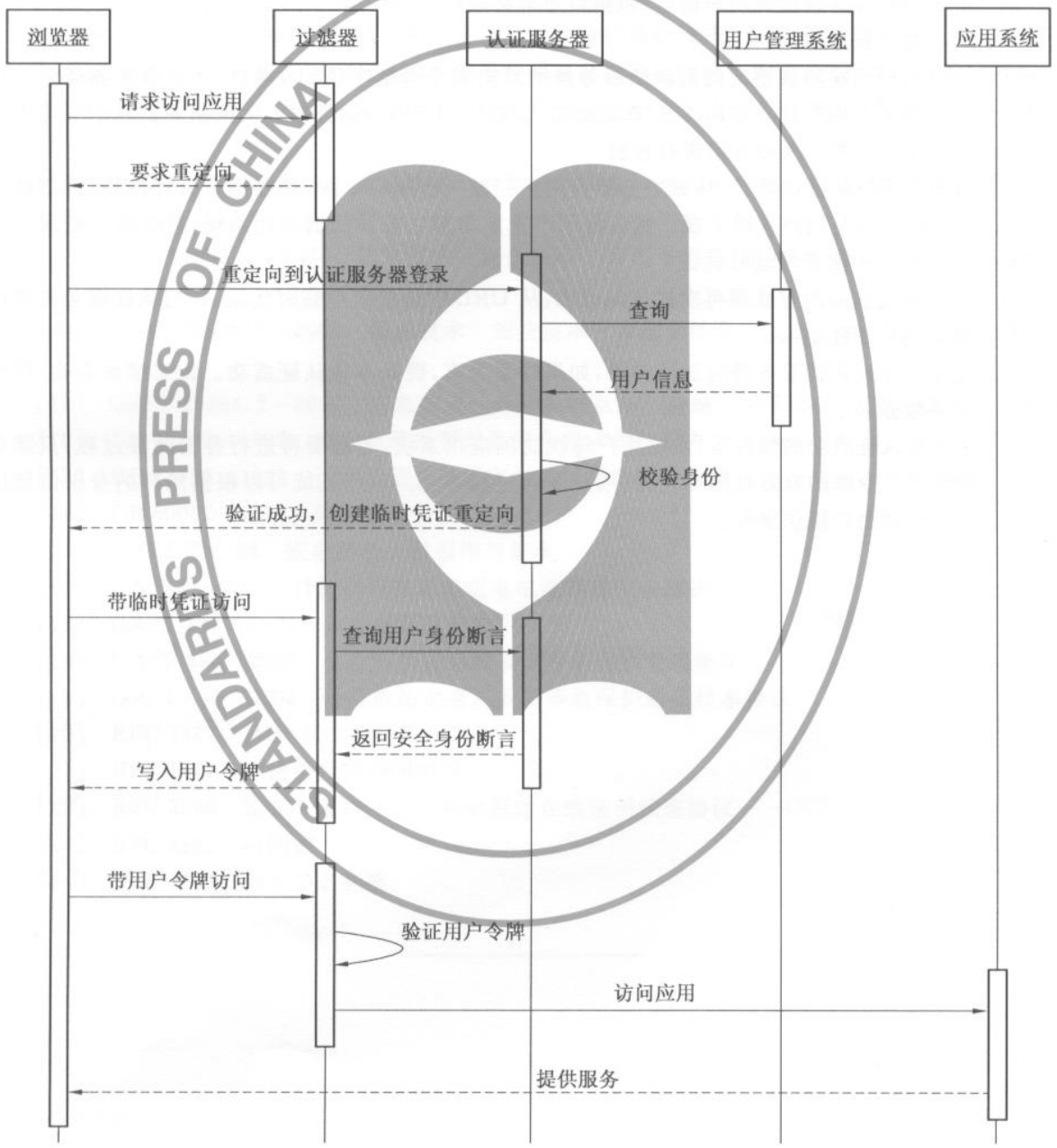

图 C.1 用户身份认证过程

C.2 用户身份认证说明

用户身份认证说明如下：

a) 用户访问应用系统，用户请求被应用系统前端的过滤器拦截，过滤器发现用户没有认证，将用户重定向到认证服务器。

b) 用户访问认证服务器的登录页面，可以选择数字证书和静态口令两种方式登录。

1) 静态口令方式：

用户通过 HTTP POST 方式将用户名和密码提交到认证服务器，认证服务器通过查询用户管理系统验证用户信息(包括口令策略等)。

2) 数字证书方式：

用户浏览器被重定向到认证服务器的双向安全套结字(SSL)端口，认证服务器通过 SSL 握手与用户建立双向 SSL 通讯信道，并提取用户的公钥证书。认证服务器从信任库中查询对应的 CA 根证书进行校验。

c) 当用户身份认证成功后，认证服务器为用户创建一个用户令牌，保存用户认证信息，并创建一个临时凭证与用户令牌关联。然后将用户重定向到之前访问的应用系统，并在统一资源定位符(URL)中附带该临时凭证。

d) 应用系统前端的过滤器再次拦截到请求，从 URL 中解析用户临时凭证，并与认证服务器通信查询用户认证结果。

e) 过滤器收到认证服务器的返回结果，如果结果为真，确认本次认证成功。如果结果为假，拒绝提供服务。

f) 在首次认证成功的情况下，之后用户每次访问应用系统，不需要再进行身份认证过程，只需要验证用户令牌的有效性即可，直到用户令牌过期为止。应用系统可以根据用户的身份信息决定是否对用户提供服务。

参 考 文 献

[1] GB 15843.1—1995 信息技术 安全技术 实体鉴别机制 第1部分:一般模型
[2] GB 15843.2—1997 信息技术 安全技术 实体鉴别 第2部分:采用对称加密算法的机制
[3] GB/T 15843.5—2005 信息技术 安全技术 实体鉴别 第5部分:使用零知识技术的机制
[4] GB/T 19713—2005 信息技术 安全技术 公钥基础设施 在线证书状态协议
[5] GB/T 19714—2005 信息技术 安全技术 公钥基础设施 证书管理协议
[6] GB/T 19771—2005 信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范
[7] GB/T 19715.1—2005 信息技术 信息技术安全管理指南 第1部分:信息技术安全概念和模型
[8] GB/T 19715.2—2005 信息技术 信息技术安全管理指南 第2部分:管理和规划信息技术安全
[9] GB/T 17902.2—2005 信息技术 安全技术 带附录的数字签名 第2部分:基于身份的机制
[10] GB/T 17902.3—2005 信息技术 安全技术 带附录的数字签名 第3部分:基于证书的机制
[11] GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架
[12] GB 16796—1997 安全防范报警设备安全要求和试验方法
[13] GB 17859—1999 计算机信息系统安全保护等级划分准则
[14] GB 50057—1994 建筑物防雷设计规范
[15] GA/T 75—94 安全防范工程程序与要求
[16] GA 267—2000 计算机信息系统雷电电磁脉冲安全防护规范
[17] GA/T 368—2001 入侵报警系统技术要求
[18] GA/T 388—2002 计算机信息系统安全等级保护管理要求
[19] GA/T 390—2002 计算机信息系统安全等级保护通用技术要求
[20] RFC 1321 MD5 报文摘要算法
[21] RFC 1777 轻量级目录访问协议
[22] RFC 2560 X.509 因特网公钥基础设施在线证书状态协议——OCSP
[23] RFC 3161 时间戳
[24] RFC 3369 数字签名标准

中华人民共和国公共安全
行业标准
城市监控报警联网系统 技术标准
第2部分:安全技术要求
GA/T 669.2—2008
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 35千字
2008年10月第一版 2008年10月第一次印刷
*
书号:155066·2-19164 定价 20.00元

GA/T 669.2-2008