中华人民共和国国家军用标准

FL 3300 GJB 6866－2009

军队数字证书中心通用要求

General requirements for military digital certification authority

2009－12－22 发布 2010－04－01 实施

中国人民解放军总装备部 批 准

前　言

本标准的附录 A 是规范性附录。

本标准由中国人民解放军总参谋部机要局提出。

本标准起草单位：总参谋部机要技术中心。

本标准主要起草人：何良生、殷荣怀、张庆广、姚家俊、陈亚岗、刘钢利。

军队数字证书中心通用要求

1　范围

本标准规定了军队数字证书中心的总体、物理环境、安全保密、运行管理要求。

本标准适用于军队数字证书中心的建设、运行和管理。

2　引用文件

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改单(不包括勘误的内容)或修订版本都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GB 50057－1994　建筑物防雷设计规范

GB 50174－1993　电子计算机机房设计规范

GJBz 20219－1994　军用电磁屏蔽室通用技术要求和检验方法

GJBz 20397－1997　密码机屏蔽机房的安装、使用和检测

GBJ 16－1987　建筑设计防火规范

GBJ 140－1990　建筑灭火器配置设计规范

《中国人民解放军数字证书认证中心管理规定(试行)》　总参谋部机要局　2005 年 6 月 15 日[2005]机字第 097 号

3　术语和定义

下列术语和定义适用于本标准。

3.1　军队数字证书中心　military digital certification authority

由军队统一授权，直接为军事信息系统提供数字证书服务的数字证书认证机构。

3.2　证书撤销列表　certificate revocation list

由证书机构签发的一个已标识的列表，是证书颁发者确认的一批无效证书。

3.3　一类数字证书中心　digital certification authority of first class

负责证书认证系统密码密钥管理，提供证书注册、签发、制作和查询服务的数字证书中心。

3.4　二类数字证书中心　digital certification authority of second class

负责提供证书注册、制作和查询服务的数字证书中心。

3.5　核心区　key area

安装数字证书认证系统各类服务器、网络设备和安全设备的区域。

3.6　值班服务区　duty service area

安装数字证书认证系统各类业务操作终端和管理终端的区域。

3.7　办公区　office area

设置办公室、会议室和辅助设施的区域。

4　数字证书中心总体要求

4.1　数字证书中心的分类

军队数字证书中心分为一类数字证书中心和二类数字证书中心。

4.2　数字证书中心设置原则

数字证书中心的设置原则为：

a) 一类数字证书中心一般设置于总部及大军区级单位的机要部门；

b) 二类数字证书中心隶属于一类数字证书中心，设置于有关单位和应用部门，可根据需要建设数字证书注册、服务和用户管理等机构。

4.3 一类数字证书中心职能

一类数字证书中心履行下列职能：

a) 负责数字证书中心的日常管理工作，执行一类数字证书中心的运行策略和管理规范；

b) 负责数字证书认证系统的运行与管理，开展数字证书服务业务(注册、审核、签发、制证、发布、变更、注销、归档等)；

c) 负责数字证书认证系统的密码管理，组织密钥分发和更换；

d) 监督检查用户部门对数字证书的使用情况，协调处理证书使用中的有关问题；

e) 对所属的二类数字证书中心的运行管理工作进行检查和指导。

4.4 二类数字证书中心职能

二类数字证书中心履行下列职能：

a) 接受对应的一类数字证书中心的业务指导，负责数字证书中心的日常管理工作，执行二类数字证书中心的运行策略和管理规范；

b) 负责数字证书认证系统的运行与管理，开展数字证书服务业务(注册、审核、制证、变更、注销等)。

4.5 人员要求

军队数字证书中心的密码管理人员，应为机要人员或符合机要人员条件；其他人员上岗前应经过机要部门组织的业务和技术培训。

4.6 岗位职责

数字证书中心根据人员岗位制定相应的岗位职责，各类工作人员应按照岗位职责开展工作。

4.7 数字证书中心区域设置及要求

数字证书中心区域划分为核心区、值班服务区和办公区，各区域的设置既要便于工作，相对集中，又要在物理位置上相对独立。

4.8 保密要求

数字证书中心应建立严格的保密制度，确保数字证书业务开展中产生和获得的信息不被泄露，其基本要求如下：

a) 任何个人不应私自复制涉密信息，因工作需要确需复制的，应经主管领导批准，二人作业，严格登记；

b) 系统程序盘、密钥盘、证书载体、身份卡等移动存储介质和相关涉密资料，应有专人负责，定期核查；

c) 发现涉密资料或载体丢失，应按要求采取措施，及时报告。

4.9 安全控制

机房、走廊应安装门禁、红外和视频监控装置，对出入人员按照权限管理，对机房、配电设施及出入口进行实时监控，出入记录和报警监控信息保存不少于30个工作日。

5 一类数字证书中心要求

5.1 物理环境要求

5.1.1 机房通用要求

一类数字证书中心应拥有独立的工作机房，其基本要求如下：

a) 机房使用面积应按公式(1)计算，实际使用面积应不小于计算结果；

$$S-kA \quad \cdots\cdots (1)$$

式中：

S ——计算机机房的面积(m^2)；

k 系数，一般取值($4.4m^2$~$5.5m^2$)/台(架)；

A ——计算机机房内所有设备的数量。

b) 机房防火设计应符合 GBJ 16－1987 的规定；

c) 机房消防器材配备应符合 GBJ 140－1990 的规定；

d) 防雷接地应符合 GB 50057－1994 的规定；

e) 机房应配备温度调节、除湿或加湿设施；

f) 机房应安装防盗、防火报警装置。

5.1.2 核心区机房

一类数字证书中心应在工作机房中设立独立的核心区机房，其基本要求如下：

a) 核心区应设在电磁屏蔽间，屏蔽指标应符合 GJBz 20397－1997 的规定；

b) 机房内应安装新风系统，通过带滤波器新风机补充新风，空调系统应有空气滤波装置，定期对滤清装置进行清洗；

c) 机房的温、湿度应符合 GB 50174－1993 中的 A 级要求。

5.1.3 值班服务区机房

一类数字证书中心应拥有独立的值班服务区机房，其基本要求如下：

a) 值班服务区机房内所有终端应放置在电磁屏蔽机桌内，电磁屏蔽机桌屏蔽指标应符合 GJBz 20219－1994 中的 B 级要求；

b) 值班服务区应明确划分工作人员操作区，外来人员未经允许不得进入操作区；

c) 机房的温、湿度应符合 GB 50174－1993 中的 B 级要求。

5.1.4 供电要求

一类数字证书中心机房供电要求如下：

a) 机房应采用集中供电方式，并提供双路市电和不间断电源，不间断电源供电时间应不小于 4h。

b) 电源为 220×(1±10%)V，50Hz。

c) 机房应设置三组接地，交流工作接地、安全工作接地和直流工作接地。交流工作接地和安全工作接地电阻值应不大于 4Ω；直流工作接地电阻值应按计算机系统具体要求确定。

5.2 安全保密要求

5.2.1 网络安全措施

数字证书认证系统网络安全措施和基本要求如下：

a) 网络节点管理：对于网络中任何节点的增加、删除、改变，应建立相应的审批和操作程序；对网络 IP 地址、主机名按照标准进行统一编码和分配，并严格保密。

b) 内网与外网隔离：内网指数字证书认证系统与军事信息网接入处以内的网络，外网指接入处以外的网络。应采取有效的技术措施划分内部网与外部网，对内外网实施网络隔离，加装防火墙。

c) 子网间隔离：在各个子系统之间，应采取有效的技术措施进行隔离。

d) 网络运行监控管理：应有入侵检测、漏洞扫描、网络防病毒和安全审计等措施，实时监控网络运行状况。

5.2.2 物理环境安全控制措施

物理环境安全控制措施如下：

a) 对计算机、服务器、安全设备、网络设备及屏蔽间等基础设施的操作应严格控制，制定安全授权策略并进行监控；

b) 对机房、走廊的安全控制同 4.9。

5.2.3 应急计划与数据安全

5.2.3.1 应急计划

数字证书中心应根据可能出现的突发事件，制定相应的应急计划，保证网络基础设施、主机系统、应用系统及数据库系统稳定运行。

5.2.3.2 数据备份

数字证书中心应采用集中统一的数据备份管理策略，确保系统安全，数据备份应满足以下要求：

a) 备份应在不中断数据库使用的前提下实施；

b) 具有本地数据备份和管理策略；

c) 具有远程备份和全局管理策略；

d) 具有备份数据的异地保存策略，异地备份的距离应不小于50km。

5.2.4 密钥的管理

5.2.4.1 根密钥的管理

根密钥的制作和使用应严格按照数字证书认证系统操作规程执行，在制作根密钥时应明确根密钥的分割份数，指定根密钥分量的保管者，根密钥制作完成后由保管者负责保管，根密钥不使用时应处于离线状态。

5.2.4.2 数字证书中心密钥的管理

数字证书中心的密钥由密码设备生成并加密存放在该密码设备中，加密后的密钥分割成三份，导出到IC卡中，由指定的保管者负责保管。

5.2.4.3 用户密钥的管理

用户密钥应存放在指定的密码载体中，用户加密密钥应在数字证书认证系统备份。

5.2.5 系统管理员权限管理

5.2.5.1 系统管理员权限分配

系统管理员的权限应分配给两名以上的人员使用，通过系统管理控制台给参与管理的人员设定口令及口令信息保存方式，由系统管理员分别保管。

5.2.5.2 系统管理员权限验证

系统管理员通过系统管理控制台对系统进行操作时，应至少有两名以上管理员在场的情况下进入系统进行操作。

5.3 运行规范要求

5.3.1 岗位设置

数字证书中心根据人员和承担的任务设置相应的岗位，人员岗位设置如下：

a) 密码管理人员；

b) 系统管理人员；

c) 安全管理人员；

d) 操作使用人员。

5.3.2 证书办理流程

军队数字证书办理流程图见附录A，办理流程如下：

a) 用户应按《中国人民解放军数字证书认证中心管理规定(试行)》如实填写《数字证书申请表》并提交数字证书业务受理机构。

b) 各数字证书业务受理机构应严格审核用户提供的证明材料和身份资料，如不合格，则注明原因并按原申请渠道退回。如合格，则签署审查意见并按照隶属关系或有关规定，提交相关数字证书中心。

c) 数字证书中心收到审核后的《数字证书申请表》，应指定人员录入申请表信息，确认无误后提交审核终端。

d) 审核未通过时，执行审核拒绝操作，重新录入，审核通过后，提交制证终端。

c） 按操作规程为用户制作证书，并对证书信息进行核对，发现错误时，将错误信息反馈给录入终端。核对无误将证书信息存档，并按规定在网上发布，制作好的证书及材料应按申请渠道尽快颁发给用户。

5.3.3 日常运行规范

数字证书中心应制定日常运行规范来保证中心的安全稳定运行，其基本运行规范如下：

a） 工作人员应遵守有关保密工作制度。

b） 建立 24h 值勤制度，值勤人员应坚守岗位，保持数字证书认证系统始终处于正常工作状态。

c） 每周应不少于两个工作日受理证书业务，签发的数字证书、证书状态信息和证书撤销列表，应在完成签发后一个工作日内发布，因网络原因不能发布的，应在三个工作日内人工发布。

d） 应制定数字证书认证系统数据备份策略，按照备份策略对数据进行备份。

e） 每月应备份一次系统的日志信息、密钥数据、审计数据等。在进行证书签发、变更、撤销等操作后，应及时进行检查核对和数据备份。

f） 每月应至少查阅一次漏洞扫描和入侵检测的结果及防火墙日志，进行一次安全审计和计算机病毒扫描，防病毒软件应定期升级，特殊情况应及时更新。

g） 应定期对机房设备进行检查，对故障设备进行维修。

h） 每年应对数字证书认证系统进行一次安全风险评估，提交安全风险评估报告。

6 二类数字证书中心要求

6.1 物理环境要求

6.1.1 机房通用要求

二类数字证书中心应有独立的工作机房，其基本要求如下：

a） 二类数字证书中心各区域机房总使用面积一般不小于 $30m^2$；

b） 机房防火设计应符合 GBJ 16－1987 的规定；

c） 机房消防器材配备应符合 GBJ 140－1990 的规定；

d） 防雷接地应符合 GB 50057－1994 的规定；

e） 数字证书系统应放置在电磁屏蔽机桌内，屏蔽机桌屏蔽指标应符合 GJBz 20219－1994 中的 B 级要求；无法使用屏蔽机桌的应安装通过军用信息安全认证的电磁信号干扰器；

f） 机房的温、湿度应符合 GB 50174－1993 中的 B 级要求；

g） 机房应安装防盗、防火报警设施。

6.1.2 核心区机房

二类数字证书中心应在工作机房中设立独立的核心区机房，其基本要求如下：

a） 核心区机房应采取有效的安全防护措施。

b） 未安装屏蔽机柜的机房内应安装电磁信号干扰器。

c） 机房应采用集中供电方式，并提供双路市电和不间断电源，不间断电源供电时间不小于 2h。

d） 机房应设置三组接地，交流工作接地、安全工作接地和直流工作接地。交流工作接地和安全工作接地电阻值应不大于 4Ω；直流工作接地电阻值应按计算机系统具体要求确定。

6.1.3 值班服务区机房

工作机房中应设置值班服务区机房，值班服务区应明确划分工作人员操作区和外来人员等待区，外来人员不应进入操作区。

6.1.4 供电要求

供电要求同 5.1.4。

6.2 安全保密要求

6.2.1 网络安全

6.2.1.1　网络隔离

应采取有效措施对内外网实施隔离，确保网络安全。

6.2.1.2　网络运行监控管理

应采用入侵检测、漏洞扫描、网络防病毒和安全审计等技术，实时监控网络运行状况。

6.2.2　应急计划与数据安全

6.2.2.1　应急计划

应根据可能出现的突发事件，制定相应的应急计划，保证网络基础设施、主机系统、应用系统及数据库运行的安全。

6.2.2.2　数据备份

应根据数字证书认证系统数据备份策略做好本地数据备份和管理。

6.3　运行规范要求

6.3.1　岗位设置

应根据承担的任务和人员情况设置人员岗位，基本人员岗位设置如下：

a)　系统管理人员；

b)　安全管理人员；

c)　操作使用人员。

6.3.2　证书办理流程

军队数字证书办理流程同5.3.2。

6.3.3　日常运行规范

二类数字证书中心应制定日常运行规范来保证中心的安全稳定运行，其基本运行规范如下：

a)　工作人员应遵守有关保密工作制度。

b)　工作人员应坚守工作岗位，认真履行职责，保持与一类数字证书中心的联络畅通，积极配合上级检查。

c)　每周受理数字证书业务的时间应不少于三个工作日，其余时间进行系统维护、检查和数据资料整理。

d)　每两月应至少备份一次系统的日志信息、审计数据等。在进行证书签发、变更、撤销等操作后，及时进行检查核对和数据备份。

e)　每月应至少查阅一次漏洞扫描和入侵检测的结果及防火墙日志，进行一次安全审计和计算机病毒扫描，防病毒软件应定期升级，特殊情况应及时更新。

附　录　A
（规范性附录）
军队数字证书办理流程

数字证书办理流程见图 A.1。

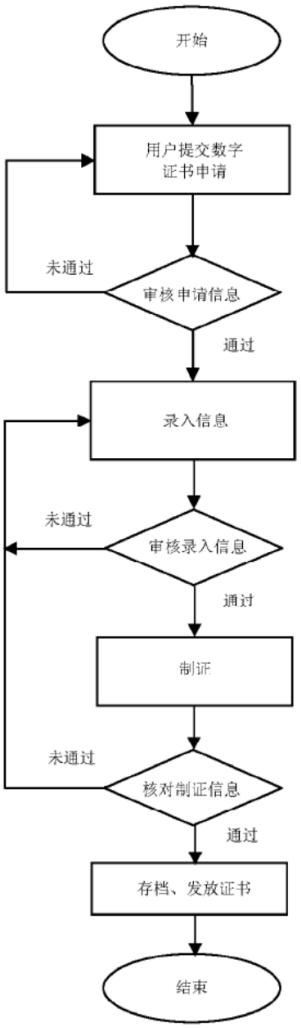

图 A.1　数字证书办理流程图

中 华 人 民 共 和 国
国家军用标准
军队数字证书中心通用要求
GJB 6866—2009
*
总装备部军标出版发行部出版
(北京东外京顺路 7 号)
总装备部军标出版发行部印刷车间印刷
总装备部军标出版发行部发行

*
开本 880×1230　1/16　印张 1　字数 21 千字
2010 年 3 月第 1 版　2010 年 3 月第 1 次印刷
印数 1—500
*
军标出字第 7914 号　定价 15.00 元