ICS 35.040
L 80

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的[redacted]。本文件的发布机[redacted]构不承担[redacted]

信息安全技术
信息系统密码应用基本要求

1 范围

本标准规

统密码应用

2 规范性引用文件

下列文件对于本文件的应用是必不可少的

凡是注日期的引用文件，仅注日期的版本适用于本文

证明一个已经发生的操作行为无法否认的性质。

3.5

加密 encipherment;encryption

对数据……文的过程。

3.6

密钥 key

控制密码算法运算的关键信息或参数。

3.7

密钥管理　key management

根据安全策略对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥生存周期的管理。

3.8

身份鉴别　identity authentication

证实一个

password

3.11

访问控制　access control

4.1.2

密码应用技术要求维度

安全机密性、完整性、真实

3） 日志记录：

访问控制信息；

5） 重要信息资源安全标记；

6） 重要可执行程序；

7）

1） 进入重要物理区域人员的身份鉴别；

2） 通信双方的身份鉴别；

3）

1） 重要可执行程序的来源真实性；

处理密码应用安

密码应用基本要求等级描述

本标准对信息系统密码应用划

为自低向高的五个等级，参照 GB/T 22239 的

度的各类要求，并鼓励使用

密码保障信息系统安全。

求的基础上，增加操作

程、人员上岗培训与考

5 通用要求

第一级到第

商用密码认证机构认证合格。

6.2 网络和通信安全

本级要求包括

商用

6.3 设备和计算

本级要求包

6.4 应用和数据安全

(c) 可采用密码技术保证信息系统应用的重要数

(d) 可采用密码技术保证信息系统应用的重要数

(e)

g） 以上almost

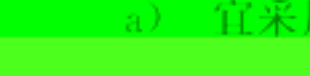
码服务，该密码服务应符合法律法规的相关要求。

被仅授受任何获益的规定

商用密码认证

解并遵守密码相关法律法规和密码规

和关人员



7 第二级密码应用基本要

7.1 物理和环境安全

本级要求包括：

a） 宜采用密码

b） 可采用密码技术保证电子门禁系统进出记录数据的存储完整性

码服务，该密码服务应符合法律法规的相关要求

f) 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

8 密钥和计算安全

本级要求包括：

a) 应采用密码技术保证重要数据在存储过程中的完整性；

b) 应依据密码相关标准和密码应用需求，制定密码应用方案。

d） 投入运行前宜进行密码应用安全性评估。

7.8 应急处置

本级要求[illegible]应用[illegible]急策略，做好应急资源[illegible]准备，当密码应用安全事件发生时，按照应急[illegible]处置措施[illegible]

8 第三级密码应用基本要求

8.1 物理和环境安全

本级[illegible]

[illegible]

[illegible]采用密码技术保证通信过程中数据的完整性；

[illegible]采用密码技术保证网络边界访问控制信息的完整性；

[illegible]采用密码技术对从外部连接的设备（如无线接入设备）进行接入认证，确保只有认证后的设备才可以接入网络；

[illegible]服务，该密码服务应符合法律

b） 宜采用密码技

f） 宜采用密码技术保证信息系统应用的

g） 宜采用密

信息系统应符合以下管理制度要求：

c）

岗位；

2） 对关键岗位建

所需专业技能；

b） 应定期对密码应用安全岗位人员进

保密合同，承担保密义务。

8.7 建设运行

d) 投入运行前

c) 应采用

g) 以上采用的密码产品，应达到 GB/T 37092 二

商用密码认证机构认证合格；

g) 以上采用的密码产品，应达到 GB/T 37092 二

商用密码认证机构认证合格；

级及以上安全要求。

9.3 设备和计算安

本级要求包括：

a) 应采用密码技术对登录

c) 应采

商用密码

的机密性；

管理制度

）应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和

）根据密码应用的实际情况，设置

员岗

位不可与密钥管理

、密码操作员兼任；

密钥管理

、密钥安全审计

码操作员应由本机构的内部员

的对

d) 应定期对密码应用安全岗位人员进行

e) 应建立关键

人员保密制度和调离制度

码管理部门进行报告；

的密钥管理部门报告事件发生情况；

第五级密码应用基本要求

略。

附 录 A
（资料性附录）
不同级别密码应用基本要求汇总列表

第一级～第四级密码应用基本要求，见表 A.1，第五级略。

表 A.1 第一级～第四级密码应用基本要求汇总列表

表 A.1（续）

			定期修订安全管理制度			应	应
			明确管理制度发布流程			应	应
			制度执行过程记录留存			应	应
			了解并遵守密码相关法律法规和密码管理制度	应	应	应	应
			建立密码应用		应		应
		管理要求	人员管理	建立上岗人员培训制度		应	应	应
				定期进行安全岗位人员考核			应	应
				建立关键岗位人员保密制度和调				

附 录 B
（资料性附录）
密钥生存周期的管理

有者、使用起始时间、使用终止时间等

止公钥被非授权篡改。

d） 密钥使用

安全性和正确性。需要注意的是

性和完整性

i) 密钥恢复

可以支持用户密钥恢复和司法密钥恢[illegible]为是审计涉及的范围，有[illegible]审计[illegible]信息，包括恢复的主体、恢复的时间等。

j) 密钥销毁

密钥销毁[illegible]要注意的是销毁[illegible]果中恢复原密钥。

参 考 文 献

[1] GB/T 22239—2019 信[illegible]术 网络安全等级保护基本要求