ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39786—2021

信息安全技术
信息系统密码应用基本要求

Information security technology—
Baseline for information system cryptography application

2021-03-09 发布　　2021-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京数字认证股份有限公司、国家密码管理局商用密码检测中心、中国科学院数据与通信保护研究教育中心、公安部第三研究所、上海交通大学、北京信息安全测评中心、成都卫士通信息产业股份有限公司、中国金融电子化公司、飞天诚信科技股份有限公司、安徽科测信息技术有限公司、深圳市网安计算机安全检测技术有限公司、山东省计算中心(国家超级计算济南中心)、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、北京电子科技学院、北京三未信安科技发展有限公司、兴唐通信科技有限公司。

本标准主要起草人:詹榜华、宋玲娓、罗鹏、邓开勇、夏鲁宁、霍炜、刘健、许长伟、田敏求、傅大鹏、马原、郑昉昱、陈广勇、黎水林、银鹰、刘芳、肖秋林、张众、李晨旸、张晓溪、杨宏志、朱鹏飞、倪又明、程苏秦、刘健、阎亚龙、高志权、钟博、张文科、刘尚焱。

信息安全技术
信息系统密码应用基本要求

1 范围

本标准规定了信息系统第一级到第四级的密码应用的基本要求，从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面提出了第一级到第四级的密码应用技术要求，并从管理制度、人员管理、建设运行和应急处置四个方面提出了第一级到第四级的密码应用管理要求。

注：第五级密码应用仅在本标准中描述通用要求，第五级密码应用技术要求和管理要求不在本标准中描述。

本标准适用于指导、规范信息系统密码应用的规划、建设、运行及测评。在本标准的基础之上，各领域与行业可结合本领域与行业的密码应用需求来指导、规范信息系统密码应用。

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件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 37092 信息安全技术 密码模块安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

机密性 confidentiality

保证信息不被泄露给非授权实体的性质。

3.2

数据完整性 data integrity

数据没有遭受以非授权方式所作的改变的性质。

3.3

真实性 authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息之类的实体。

3.4

不可否认性 non-repudiation

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

对数据进行密码变换以产生密文的过程。

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、恢复和销毁等密钥全生存周期的管理。

3.8

身份鉴别　identity authentication

证实一个实体所声称身份的过程。

3.9

消息鉴别码　message authentication code

利用对称密码技术或密码杂凑技术，在秘密密钥参与下，由消息所导出的数据项。任何持有这一秘密密钥的实体，可利用消息鉴别码检查消息的完整性和始发者身份。

3.10

动态口令　one-time password

基于时间、事件等方式动态生成的一次性口令。

3.11

访问控制　access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

4　概述

4.1　信息系统密码应用技术框架

4.1.1　框架概述

本标准从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出密码应用技术要求，保障信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性；并从信息系统的管理制度、人员管理、建设运行和应急处置四个方面提出密码应用管理要求，为信息系统提供管理方面的密码应用安全保障。

4.1.2　密码应用技术要求维度

技术要求主要由机密性、完整性、真实性、不可否认性四个密码安全功能维度构成，具体保护对象或应用场景描述如下：

a）　机密性技术要求保护对象

使用密码技术的加解密功能实现机密性，信息系统中保护的对象为：

1）　身份鉴别信息；

2）　密钥数据；

3）　传输的重要数据；

4）　信息系统应用中所有存储的重要数据。

b）　完整性技术要求保护对象

使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现完整性，信息系统中保护的对象为：

1）　身份鉴别信息；

2）　密钥数据；

3） 日志记录；
4） 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） 视频监控音像记录；
8） 电子门禁系统进出记录；
9） 传输的重要数据；
10） 信息系统应用中所有存储的重要数据。

c） 真实性技术要求应用场景

使用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现真实性，信息系统中应用场景为：

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） 网络设备接入时的身份鉴别；
4） 重要可执行程序的来源真实性保证；
5） 登录操作系统和数据库系统的用户身份鉴别；
6） 应用系统的用户身份鉴别。

d） 不可否认性技术要求保护对象

使用基于公钥密码算法的数字签名机制等密码技术来保证数据原发行为的不可否认性和数据接收行为的不可否认性。

4.1.3 密码应用管理要求维度

管理要求由管理制度、人员管理、建设运行、应急处置等四个密码应用管理维度构成，具体如下：

a） 密码应用安全管理相关流程制度的制定、发布、修订的规范性要求；
b） 密码相关安全人员的密码安全意识以及关键密码安全岗位员工的密码安全能力的培养，人员工作流程要求等；
c） 建设运行过程中密码应用安全要求及方案落地执行的一致性和有效性要求；
d） 处理密码应用安全相关的应急突发事件的能力要求。

4.2 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分为自低向高的五个等级，参照 GB/T 22239 的等级保护对象应具备的基本安全保护能力要求，本标准提出密码保障能力逐级增强的要求，用一、二、三、四、五表示。信息系统管理者可按照业务实际情况选择相应级别的密码保障技术能力及管理能力，各等级描述如下：

——第一级，是信息系统密码应用安全要求等级的最低等级，要求信息系统符合通用要求和最低限度的管理要求，并鼓励使用密码保障信息系统安全；
——第二级，是在第一级要求的基础上，增加操作规程、人员上岗培训与考核、应急预案等管理要求，并要求优先选择使用密码保障信息系统安全；
——第三级，是在第二级要求的基础上，增加对真实性、机密性的技术要求以及全部的管理要求；
——第四级，是在第三级要求的基础上，增加对完整性、不可否认性的技术要求；
——第五级（略）。

本标准所要求的不同等级密码应用基本要求简表参见附录 A。

5 通用要求

第一级到第五级的信息系统应符合以下通用要求：

a) 信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

b) 信息系统中使用的密码技术应遵循密码相关国家标准和行业标准；

c) 信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。

6 第一级密码应用基本要求

6.1 物理和环境安全

本级要求包括：

a) 可采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；

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；

c) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经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：

a) 可采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b) 可采用密码技术保证通信过程中数据的完整性；

c) 可采用密码技术保证通信过程中重要数据的机密性；

d) 可采用密码技术保证网络边界访问控制信息的完整性；

e) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

6.3 设备和计算安全

本级要求包括：

a) 可采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；

b) 可采用密码技术保证系统资源访问控制信息的完整性；

c) 可采用密码技术保证日志记录的完整性；

d) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

6.4 应用和数据安全

本级要求包括：

a) 可采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

b) 可采用密码技术保证信息系统应用的访问控制信息的完整性；

c) 可采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；

d) 可采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；

e) 可采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；

f) 可采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；

g) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

6.5 管理制度

使用密码技术的信息系统应符合以下管理制度要求：

a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
b) 应根据密码应用方案建立相应密钥管理规则。

6.6 人员管理

使用密码技术的信息系统应符合以下人员管理要求：

a) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
b) 应及时终止离岗人员的所有密码应用相关的访问权限、操作权限。

6.7 建设运行

本级要求包括：

a) 应依据密码相关标准和密码应用需求，制定密码应用方案；
b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照附录 B；
c) 应按照密码应用方案实施建设；
d) 投入运行前可进行密码应用安全性评估。

6.8 应急处置

本级要求为：可根据密码产品提供的安全策略，由用户自主处置密码应用安全事件。

7 第二级密码应用基本要求

7.1 物理和环境安全

本级要求包括：

a) 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
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；
c) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
d) 以上采用的密码产品，应达到 GB/T 37092 一级及以上安全要求。

7.2 网络和通信安全

本级要求包括：

a) 宜采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
b) 可采用密码技术保证通信过程中数据的完整性；
c) 宜采用密码技术保证通信过程中重要数据的机密性；
d) 可采用密码技术保证网络边界访问控制信息的完整性；
e) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

f) 以上采用的密码产品，应达到 GB/T 37092 一级及以上安全要求。

7.3 设备和计算安全

本级要求包括：

a) 宜采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
b) 可采用密码技术保证系统资源访问控制信息的完整性；
c) 可采用密码技术保证日志记录的完整性；
d) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
e) 以上采用的密码产品，应达到 GB/T 37092 一级及以上安全要求。

7.4 应用和数据安全

本级要求包括：

a) 宜采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；
b) 可采用密码技术保证信息系统应用的访问控制信息的完整性；
c) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
d) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
e) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
f) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
g) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
h) 以上采用的密码产品，应达到 GB/T 37092 一级及以上安全要求。

7.5 管理制度

使用密码技术的信息系统应符合以下管理制度要求：

a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
b) 应根据密码应用方案建立相应密钥管理规则；
c) 应对管理人员或操作人员执行的日常管理操作建立操作规程。

7.6 人员管理

使用密码技术的信息系统应符合以下人员管理要求：

a) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
b) 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权限；
c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
d) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

7.7 建设运行

本级要求包括：

a) 应依据密码相关标准和密码应用需求，制定密码应用方案；
b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照附录 B；
c) 应按照应用方案实施建设；

d） 投入运行前宜进行密码应用安全性评估。

7.8 应急处置

本级要求为：应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，按照应急处置措施结合实际情况及时处置。

8 第三级密码应用基本要求

8.1 物理和环境安全

本级要求包括：

a） 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；

b） 宜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；

c） 宜采用密码技术保证视频监控音像记录数据的存储完整性；

d） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

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

8.2 网络和通信安全

本级要求包括：

a） 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b） 宜采用密码技术保证通信过程中数据的完整性；

c） 应采用密码技术保证通信过程中重要数据的机密性；

d） 宜采用密码技术保证网络边界访问控制信息的完整性；

e） 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性；

f） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经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 二级及以上安全要求。

8.3 设备和计算安全

本级要求包括：

a） 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；

b） 远程管理设备时，应采用密码技术建立安全的信息传输通道；

c） 宜采用密码技术保证系统资源访问控制信息的完整性；

d） 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；

e） 宜采用密码技术保证日志记录的完整性；

f） 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；

g） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

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

8.4 应用和数据安全

本级要求包括：

a） 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

b） 宜采用密码技术保证信息系统应用的访问控制信息的完整性；
c） 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
d） 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
e） 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
f） 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
g） 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
h） 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；
i） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
j） 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

8.5 管理制度

使用密码技术的信息系统应符合以下管理制度要求：

a） 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
b） 应根据密码应用方案建立相应密钥管理规则；
c） 应对管理人员或操作人员执行的日常管理操作建立操作规程；
d） 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
e） 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
f） 应具有密码应用操作规程的相关执行记录并妥善保存。

8.6 人员管理

使用密码技术的信息系统应符合以下人员管理要求：

a） 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
b） 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权限：
   1） 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；
   2） 对关键岗位建立多人共管机制；
   3） 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；
   4） 相关设备与系统的管理和使用账号不得多人共用。
c） 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
d） 应定期对密码应用安全岗位人员进行考核；
e） 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

8.7 建设运行

本级要求包括：

a） 应依据密码相关标准和密码应用需求，制定密码应用方案；
b） 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照附录 B；
c） 应按照应用方案实施建设；

d) 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
e) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

8.8 应急处置

本级要求包括：
a) 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
b) 事件发生后，应及时向信息系统主管部门进行报告；
c) 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

9 第四级密码应用基本要求

9.1 物理和环境安全

本级要求包括：
a) 应采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
b) 应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；
c) 应采用密码技术保证视频监控音像记录数据的存储完整性；
d) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
e) 以上采用的密码产品，应达到 GB/T 37092 三级及以上安全要求。

9.2 网络和通信安全

本级要求包括：
a) 应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性；
b) 应采用密码技术保证通信过程中数据的完整性；
c) 应采用密码技术保证通信过程中重要数据的机密性；
d) 应采用密码技术保证网络边界访问控制信息的完整性；
e) 宜采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性；
f) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经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 三级及以上安全要求。

9.3 设备和计算安全

本级要求包括：
a) 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
b) 远程管理设备时，应采用密码技术建立安全的信息传输通道；
c) 应采用密码技术保证系统资源访问控制信息的完整性；
d) 应采用密码技术保证设备中的重要信息资源安全标记的完整性；
e) 应采用密码技术保证日志记录的完整性；
f) 应采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；
g) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经

商用密码认证机构认证合格；

h） 以上采用的密码产品，应达到 GB/T 37092 三级及以上安全要求。

9.4 应用和数据安全

本级要求包括：

a） 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

b） 应采用密码技术保证信息系统应用的访问控制信息的完整性；

c） 应采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；

d） 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；

e） 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；

f） 应采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；

g） 应采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；

h） 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；

i） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

j） 以上采用的密码产品，应达到 GB/T 37092 三级及以上安全要求。

9.5 管理制度

使用密码技术的信息系统应符合以下管理制度要求：

a） 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；

b） 应根据密码应用方案建立相应密钥管理规则；

c） 应对管理人员或操作人员执行的日常管理操作建立操作规程；

d） 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；

e） 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；

f） 应具有密码应用操作规程的相关执行记录并妥善保存。

9.6 人员管理

使用密码技术的信息系统应符合以下人员管理要求：

a） 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；

b） 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权限：

1） 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；

2） 对关键岗位建立多人共管机制；

3） 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；

4） 相关设备与系统的管理和使用账号不得多人共用；

5） 密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任，并应在任前对其进行背景调查。

c） 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；

d) 应定期对密码应用安全岗位人员进行考核；
e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

9.7 建设运行

本级要求包括：
a) 应依据密码相关标准和密码应用需求，制定密码应用方案；
b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照附录 B；
c) 应按照应用方案实施建设；
d) 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
e) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

9.8 应急处置

本级要求包括：
a) 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
b) 事件发生后，应及时向信息系统主管部门及归属的密码管理部门进行报告；
c) 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

10 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

指标体系			第一级	第二级	第三级	第四级
技术要求	物理和环境安全	身份鉴别	可	宜	宜	应
		电子门禁记录数据存储完整性	可	可	宜	应
		视频监控记录数据存储完整性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	网络和通信安全	身份鉴别	可	宜	应	应
		通信数据完整性	可	可	宜	应
		通信过程中重要数据的机密性	可	宜	应	应
		网络边界访问控制信息的完整性	可	可	宜	应
		安全接入认证	—	—	可	宜
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	设备和计算安全	身份鉴别	可	宜	应	应
		远程管理通道安全	—	—	应	应
		系统资源访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		日志记录完整性	可	可	宜	应
		重要可执行程序完整性、重要可执行程序来源真实性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	应用和数据安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		重要数据传输机密性	可	宜	应	应
		重要数据存储机密性	可	宜	应	应
		重要数据传输完整性	可	宜	宜	应
		重要数据存储完整性	可	宜	宜	应
		不可否认性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上

表 A.1（续）

指标体系			第一级	第二级	第三级	第四级
管理要求	管理制度	具备密码应用安全管理制度	应	应	应	应
		密钥管理规则	应	应	应	应
		建立操作规程	—	应	应	应
		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
	人员管理	了解并遵守密码相关法律法规和密码管理制度	应	应	应	应
		建立密码应用岗位责任制度	—	应	应	应
		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离制度	应	应	应	应
	建设运行	制定密码应用方案	应	应	应	应
		制定密钥安全管理策略	应	应	应	应
		制定实施方案	应	应	应	应
		投入运行前进行密码应用安全性评估	可	宜	应	应
		定期开展密码应用安全性评估及攻防对抗演习	—	—	应	应
	应急处置	应急策略	可	应	应	应
		事件处置	—	—	应	应
		向有关主管部门上报处置情况	—	—	应	应

附 录 B
（资料性附录）
密钥生存周期管理

密钥管理对于保证密钥全生存周期的安全性是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，可以保证公钥不被非授权的修改和替换。信息系统的应用和数据层面的密钥体系由业务系统根据密码应用需求在密码应用方案中明确，并在密码应用实施中落实。密钥管理包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。以下给出各个环节的密钥管理建议供参考：

a） 密钥产生

密钥可以以随机产生、协商产生等不同的方式来产生。密钥在符合 GB/T 37092 的密码产品中产生是十分必要的，产生的同时可在密码产品中记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等。

b） 密钥分发

密钥分发是密钥从一个密码产品传递到另一个密码产品的过程，分发时要注意抗截取、篡改、假冒等攻击，保证密钥的机密性、完整性以及分发者、接收者身份的真实性等。

c） 密钥存储

密钥不以明文方式存储在密码产品外部是十分必要的，并采取严格的安全防护措施，防止密钥被非授权的访问或篡改。

公钥是例外，可以以明文方式在密码产品外存储、传递和使用，但有必要采取安全防护措施，防止公钥被非授权篡改。

d） 密钥使用

每个密钥一般只有单一的用途，明确用途并按用途正确使用是十分必要的。密钥使用环节需要注意的安全问题是：使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全措施防止密钥的泄露和替换等。另外，有必要为密钥设定更换周期，并采取有效措施保证密钥更换时的安全性。

e） 密钥更新

密钥更新发生在密钥超过使用期限、已泄露或存在泄露风险时，根据相应的更新策略进行更新。

f） 密钥归档

如果信息系统中有密钥归档需求，则根据实际安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。需要注意的是，归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。如果执行密钥归档，则有必要生成审计信息，包括归档的密钥、归档的时间等。

g） 密钥撤销

密钥撤销一般针对公钥证书所对应的密钥。当证书到期后，密钥自然撤销；也可以按需进行密钥撤销，撤销后的密钥不再具备使用效力。

h） 密钥备份

对于需要备份的密钥，采用安全的备份机制对密钥进行备份是必要的，以确保备份密钥的机密性和完整性，这与密钥存储的要求是一致的。密钥备份行为是审计涉及的范围，有必要生成审计信息，包括备份的主体、备份的时间等。

i） 密钥恢复

可以支持用户密钥恢复和司法密钥恢复。密钥恢复行为是审计涉及的范围，有必要生成审计信息，包括恢复的主体、恢复的时间等。

j） 密钥销毁

密钥销毁要注意的是销毁过程的不可逆，即无法从销毁结果中恢复原密钥。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求