ICS 35.040
L 80
备案号：61709—2018

GM

中华人民共和国密码行业标准

GM/T 0054—2018

信息系统密码应用基本要求

General requirements for information system cryptography application

2018-02-08 发布　　2018-02-08 实施

国家密码管理局　　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。

本标准由密码行业标准化技术委员会提出并归口。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

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、成都卫士通信息产业股份有限公司、长春吉大正元信息技术股份有限公司、中国金融电子化公司、上海交通大学、长沙银河网络有限公司。

本标准起草人：詹榜华、邓开勇、傅大鹏、钟博、阎世杰、傅勇、阎夏强、高振鹏、胡建勋、黄一飞、张众、银鹰、周志洪、李继红、董桂斋。

引　言

密码技术作为网络安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是保障网络空间安全的关键技术。

本标准主要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了等级保护不同级别的密码技术应用要求，明确了等级保护不同级别的密钥管理和安全管理要求。

本标准中，“密码”是指“商用密码”。

本标准文本中，“可”表示可以、允许，是陈述型描述，表示在标准的界限内所允许的条款；“宜”表示推荐、建议，是推荐型描述，表示该条款是首选但不是必须要求；“应”表示应该、要求，是要求型描述，表明符合标准需要满足的要求。

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商用密码应用的基本要求。

本标准适用于指导、规范和评估信息系统中的商用密码应用。

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。

GM/T 0005 随机性检测规范

GM/T 0028 密码模块安全技术要求

GM/T 0036 采用非接触卡的门禁系统密码应用技术指南

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GM/Z 4001—2013 中的一些术语和定义。

3.1

动态口令 one-time-password；OTP；dynamic password

基于时间、事件等方式动态生成的一次性口令。

3.2

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。

3.3

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.4

加密 encipherment；encryption

对数据进行密码变换以产生密文的过程。

3.5

解密 decipherment；decryption

加密过程对应的逆过程。

3.6

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.7

密钥 key

控制密码算法运算的关键信息或参数。

3.8

密钥管理　key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

3.9

身份鉴别　authentication

确认一个实体所声称身份的过程。

3.10

数字签名　digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.11

完整性　data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.12

消息鉴别码　message authentication code；MAC

消息鉴别算法的输出，又称消息认证码。

3.13

真实性　authenticity

确保主体或资源的身份正是所声称的特性。真实性适用于用户、进程、系统和信息之类的实体。

3.14

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。

4　缩略语

下列缩略语适用于本文件。

MAC　消息鉴别码(Message Authentication Code)

5　总体要求

5.1　密码算法

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

5.2　密码技术

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。

5.3　密码产品

信息系统中使用的密码产品与密码模块应通过国家密码管理部门核准。

5.4　密码服务

信息系统中使用的密码服务应通过国家密码管理部门许可。

6 密码功能要求

6.1 机密性

使用密码加密功能实现机密性，信息系统中保护的对象为：

a) 传输的重要数据、敏感信息数据或整个报文；
b) 存储的重要数据和敏感信息数据；
c) 身份鉴别信息；
d) 密钥数据。

6.2 完整性

使用消息鉴别码(MAC)或数字签名实现完整性，信息系统中保护的对象为：

a) 传输的重要数据、敏感信息数据或整个报文；
b) 存储的重要数据、文件和敏感信息数据；
c) 身份鉴别信息；
d) 密钥数据；
e) 日志记录；
f) 访问控制信息；
g) 重要信息资源敏感标记；
h) 重要程序；
i) 采用可信计算技术建立从系统到应用的信任链；
j) 视频监控音像记录；
k) 电子门禁系统进出记录。

6.3 真实性

使用对称加密、动态口令、数字签名等实现真实性，信息系统中应用场景为：

a) 进入重要物理区域人员的身份鉴别；
b) 通信双方的身份鉴别；
c) 网络设备接入时的身份鉴别；
d) 采用可信计算技术的平台身份鉴别；
e) 登录操作系统和数据库系统的用户身份鉴别；
f) 应用系统的用户身份鉴别。

6.4 不可否认性

使用数字签名等密码技术实现实体行为的不可否认性，针对在信息系统中所有需要无法否认的行为，包括发送、接收、审批、创建、修改、删除、添加、配置等操作。

7 密码技术应用要求

7.1 物理和环境安全

7.1.1 总则

物理和环境安全密码应用总则如下：

a) 采用密码技术实施对重要场所、监控设备等的物理访问控制；
b) 采用密码技术对物理访问控制记录、监控信息等物理和环境的敏感信息数据实施完整性保护；
c) 采用密码技术实现的电子门禁系统应遵循 GM/T 0036。

7.1.2 等级保护第一级信息系统

第一级信息系统要求如下：
a) 可使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；
b) 可使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性。

7.1.3 等级保护第二级信息系统

第二级信息系统要求如下：
a) 宜使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；
b) 宜使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性；
c) 宜采用符合 GM/T 0028 的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.1.4 等级保护第三级信息系统

第三级信息系统要求如下：
a) 应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；
b) 应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性；
c) 应使用密码技术的完整性功能来保证视频监控音像记录的完整性；
d) 宜采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.1.5 等级保护第四级信息系统

第四级信息系统要求如下：
a) 应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；
b) 应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性；
c) 应使用密码技术的完整性功能来保证视频监控音像记录的完整性；
d) 应采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.2 网络和通信安全

7.2.1 总则

网络和通信安全密码应用总则如下：
a) 采用密码技术对连接到内部网络的设备进行安全认证；
b) 采用密码技术对通信的双方身份进行认证；
c) 采用密码技术保证通信过程中数据的完整性；

d) 采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；
e) 采用密码技术保证网络边界访问控制信息、系统资源访问控制信息的完整性；
f) 采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

7.2.2 等级保护第一级信息系统

第一级信息系统要求如下：

a) 可在通信前基于密码技术进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；
b) 可使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性；
c) 可采用密码技术保证通信过程中数据的完整性；
d) 可采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性。

7.2.3 等级保护第二级信息系统

第二级信息系统要求如下：

a) 宜在通信前基于密码技术进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；
b) 宜使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性；
c) 宜采用密码技术保证通信过程中数据的完整性；
d) 宜采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；
e) 宜采用符合 GM/T 0028 的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.2.4 等级保护第三级信息系统

第三级信息系统要求如下：

a) 应在通信前基于密码技术对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；
b) 应使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性；
c) 应采用密码技术保证通信过程中数据的完整性；
d) 应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；
e) 应采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理；
f) 宜采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.2.5 等级保护第四级信息系统

第四级信息系统要求如下：

a) 应在通信前基于密码技术对通信双方进行验证或认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；
b) 应采用密码技术对连接到内部网络的设备进行身份认证，确保接入网络的设备真实可信；
c) 应使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性；
d) 应采用密码技术保证通信过程中数据的完整性；

e) 应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；
f) 应采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理；
g) 应基于符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.3 设备和计算安全

7.3.1 总则

设备和计算安全密码应用总则如下：
a) 采用密码技术对登录的用户进行身份鉴别；
b) 采用密码技术的完整性功能来保证系统资源访问控制信息的完整性；
c) 采用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；
d) 采用密码技术的完整性功能对重要程序或文件进行完整性保护；
e) 采用密码技术的完整性功能来对日志记录进行完整性保护。

7.3.2 等级保护第一级信息系统

第一级信息系统要求如下：
a) 可使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，使用密码技术的真实性功能来实现鉴别信息的防假冒；
b) 可使用密码技术的完整性功能来保证系统资源访问控制信息的完整性；
c) 可使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；
d) 可使用密码技术的完整性功能来对日志记录进行完整性保护。

7.3.3 等级保护第二级信息系统

第二级信息系统要求如下：
a) 宜使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，宜使用密码技术的真实性功能来实现鉴别信息的防假冒；
b) 在远程管理时，宜使用密码技术的机密性功能来实现鉴别信息的防窃听；
c) 宜使用密码技术的完整性功能来保证系统资源访问控制信息的完整性；
d) 宜使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；
e) 宜使用密码技术的完整性功能来对日志记录进行完整性保护；
f) 宜采用符合 GM/T 0028 的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.3.4 等级保护第三级信息系统

第三级信息系统要求如下：
a) 应使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b) 在远程管理时，应使用密码技术的机密性功能来实现鉴别信息的防窃听；
c) 应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性；
d) 应使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；
e) 应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整

性保护；

f) 应使用密码技术的完整性功能来对日志记录进行完整性保护；

g) 宜采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.3.5 等级保护第四级信息系统

第四级信息系统要求如下：

a) 应使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 在远程管理时，应使用密码技术的机密性功能来实现鉴别信息的防窃听；

c) 应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性；

d) 应使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；

e) 应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护；

f) 应使用密码技术的完整性功能来对日志记录进行完整性保护；

g) 应采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.4 应用和数据安全

7.4.1 总则

应用和数据安全密码应用总则如下：

a) 采用密码技术对登录用户进行身份鉴别；

b) 采用密码技术的完整性功能来保证系统资源访问控制信息的完整性；

c) 采用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；

d) 采用密码技术保证重要数据在传输过程中的机密性、完整性；

e) 采用密码技术保证重要数据在存储过程中的机密性、完整性；

f) 采用密码技术对重要程序的加载和卸载进行安全控制；

g) 采用密码技术实现实体行为的不可否认性；

h) 采用密码技术的完整性功能来对日志记录进行完整性保护。

7.4.2 等级保护第一级信息系统

第一级信息系统要求如下：

a) 可使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；

b) 可使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；

c) 可采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

d) 可采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

e) 可采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；

f) 可采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；
g) 可使用密码技术的完整性功能来实现对日志记录完整性的保护。

7.4.3 等级保护第二级信息系统

第二级信息系统要求如下：

a) 宜使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；
b) 宜使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；
c) 宜采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；
d) 宜采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；
e) 宜采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；
f) 宜采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；
g) 宜使用密码技术的完整性功能来实现对日志记录完整性的保护；
h) 宜采用符合 GM/T 0028 的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.4.4 等级保护第三级信息系统

第三级信息系统要求如下：

a) 应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；
b) 应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；
c) 应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；
d) 应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；
e) 应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；
f) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；
g) 应使用密码技术的完整性功能来实现对日志记录完整性的保护；
h) 应采用密码技术对重要应用程序的加载和卸载进行安全控制；
i) 宜采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

7.4.5 等级保护第四级信息系统

第四级信息系统要求如下：

a) 应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；
b) 应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；
c) 应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；
d) 应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；
e) 应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；
f) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；
g) 应使用密码技术的完整性功能来实现对日志记录完整性的保护；
h) 应采用密码技术对重要应用程序的加载和卸载进行安全控制；
i) 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；
j) 应采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

8 密钥管理

8.1 总则

信息系统密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程。

8.2 等级保护第一级信息系统

第一级信息系统密钥管理至少包括密钥的生成、存储和使用三个过程，并满足：

a) 密钥生成
产生的密钥不能重复，并要保证其机密性。
b) 密钥存储
采取必要的安全防护措施，防止密钥被非授权获取。
c) 密钥使用
采取必要的安全防护措施，防止密钥被非法使用。

8.3 等级保护第二级信息系统

第二级信息系统密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份与恢复等过程，并满足：

a) 密钥生成
密钥的生成使用的随机数应符合 GM/T 0005 要求，密钥应在符合 GM/T 0028 的密码模块中产生。
b) 密钥存储
密钥应加密存储，并采取必要的安全防护措施，防止密钥被非法获取。
c) 密钥分发

密钥分发应采取安全措施，防止在分发过程中泄露。

d) 密钥导入与导出

应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

e) 密钥使用

密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。

f) 密钥备份与恢复

应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复。

8.4 等级保护第三级信息系统

第三级信息系统密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程，并满足：

a) 密钥生成

密钥生成使用的随机数应符合 GM/T 0005 要求，密钥应在符合 GM/T 0028 的密码模块中产生；密钥应在密码模块内部产生，不得以明文方式出现在密码模块之外；应具备检查和剔除弱密钥的能力。

b) 密钥存储

密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在符合 GM/T 0028 的二级及以上密码模块中。

c) 密钥分发

密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

d) 密钥导入与导出

应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

e) 密钥使用

密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；密钥泄露时，应停止使用，并启动相应的应急处理和响应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。

f) 密钥备份与恢复

应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

g) 密钥归档

应采取有效的安全措施，保证归档密钥的安全性和正确性；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；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

h) 密钥销毁

应具有在紧急情况下销毁密钥的措施。

8.5 等级保护第四级信息系统

第四级信息系统密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销

毁等环节进行管理和策略制定的全过程，并满足：

a） 密钥生成

应使用国家密码管理部门批准的硬件物理噪声源产生随机数；密钥应在密码设备内部产生，不得以明文方式出现在密码设备之外；应具备检查和剔除弱密钥的能力；应生成密钥审计信息，密钥审计信息包括：种类、长度、拥有者信息、使用起始时间、使用终止时间。

b） 密钥存储

密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥、用户签名私钥应存储在符合 GM/T 0028 的三级及以上密码模块中或通过国家密码管理部门核准的硬件密码产品；应具有密钥泄露时的应急处理和响应措施。

c） 密钥分发

密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

d） 密钥导入与导出

应采取有效的安全措施，保证密钥导入与导出的安全，以及密钥的正确性；应采用密钥分量的方式或者专用设备的方式；应保证系统密码服务不间断。

e） 密钥使用

密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；密钥泄露时，应停止使用，并启动相应的应急处理和响应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。

f） 密钥备份与恢复

应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息应包括备份或恢复的主体、备份或恢复的时间等。

g） 密钥归档

应采取有效的安全措施，保证归档密钥的安全性和正确性；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；密钥归档应进行记录，并生成审计信息；审计信息应包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

h） 密钥销毁

应具有在紧急情况下销毁密钥的措施。

9 安全管理

9.1 制度

9.1.1 等级保护第一级信息系统

第一级信息系统要求如下：

a） 可制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容；

b） 可定期对密码安全管理制度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的安全管理制度进行修订。

9.1.2 等级保护第二级信息系统

第二级信息系统要求如下：

a) 宜制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容；
b) 宜定期对密码安全管理制度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的安全管理制度进行修订；
c) 宜明确相关管理制度发布流程。

9.1.3 等级保护第三级信息系统

第三级信息系统要求如下：

a) 应制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容；
b) 应定期对密码安全管理制度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的安全管理制度进行修订；
c) 应明确相关管理制度发布流程。

9.1.4 等级保护第四级信息系统

第四级信息系统要求如下：

a) 应制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容；
b) 定期对密码安全管理制度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的安全管理制度进行修订；
c) 应明确相关管理制度发布流程；
d) 制度执行过程应留存相关执行记录。

9.2 人员

9.2.1 等级保护第一级信息系统

第一级信息系统要求如下：

a) 应了解并遵守密码相关法律法规；
b) 应能够正确使用密码产品。

9.2.2 等级保护第二级信息系统

第二级信息系统要求如下：

a) 应了解并遵守密码相关法律法规；
b) 应能够正确使用密码产品；
c) 应建立相应的岗位责任制度，明确相关人员在安全系统中的职责和权限；
d) 应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；
e) 应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

9.2.3 等级保护第三级信息系统

第三级信息系统要求如下：

a) 应了解并遵守密码相关法律法规；
b) 应能够正确使用密码产品；
c) 应根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审

计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用；

d) 应建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度；

e) 应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；

f) 应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

9.2.4 等级保护第四级信息系统

第四级信息系统要求如下：

a) 应了解并遵守密码相关法律法规；

b) 应能够正确使用密码产品；

c) 应根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责应建立多人共管制度，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用；

d) 密钥管理员、密码设备操作人员应从本机构在编的正式员工中选拔，并进行背景调查；

e) 应建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度；

f) 应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；

g) 应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

9.3 实施

9.3.1 规划

9.3.1.1 等级保护第一级信息系统

信息系统规划阶段，责任单位可依据密码相关标准，制定密码应用方案。

9.3.1.2 等级保护第二级信息系统

信息系统规划阶段，责任单位宜依据密码相关标准，制定密码应用方案。

9.3.1.3 等级保护第三级信息系统

信息系统规划阶段，责任单位应依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。

通过专家审定后的方案应作为建设、验收和测评的重要依据。

9.3.1.4 等级保护第四级信息系统

信息系统规划阶段，责任单位应依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。

通过专家审定后的方案应作为建设、验收和测评的重要依据。

9.3.2 建设

9.3.2.1 等级保护第一级信息系统

可按照国家相关标准，制定密码实施方案。

9.3.2.2 等级保护第二级信息系统

宜按照国家相关标准，制定密码实施方案。

9.3.2.3 等级保护第三级信息系统

第三级信息系统要求如下：

a) 应按照国家相关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、密码系统设计方案、密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、密码系统安全管理与维护策略、密码系统实施计划等；

b) 应选用的经国家密码管理部门核准的密码产品、许可的密码服务。

9.3.2.4 等级保护第四级信息系统

第四级信息系统要求如下：

a) 应按照国家相关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、密码系统设计方案、密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、密码系统安全管理与维护策略、密码系统实施计划等；

b) 应选用的经国家密码管理部门核准的密码产品、许可的密码服务。

9.3.3 运行

9.3.3.1 等级保护第一级信息系统

信息系统投入运行前，责任单位可组织进行密码安全性评估。

9.3.3.2 等级保护第二级信息系统

信息系统投入运行前，责任单位宜组织进行密码安全性评估。

9.3.3.3 等级保护第三级信息系统

第三级信息系统要求如下：

a) 信息系统投入运行前，应经密码测评机构进行安全性评估，评估通过方可投入正式运行；

b) 信息系统投入运行后，责任单位每年应委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，应停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。

9.3.3.4 等级保护第四级信息系统

第四级信息系统要求如下：

a) 信息系统投入运行前，应经密码测评机构进行安全性评估，评估通过方可投入正式运行；

b) 信息系统投入运行后，责任单位每年应委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，应停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。

9.4 应急

9.4.1 等级保护第一级信息系统

根据密码产品提供的安全策略，由用户自主处置密码安全事件。

9.4.2 等级保护第二级信息系统

制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置。

9.4.3 等级保护第三级信息系统

第三级信息系统要求如下：

a) 制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；

b) 事件发生后，应及时向信息系统的上级主管部门进行报告；

c) 事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。

9.4.4 等级保护第四级信息系统

第四级信息系统要求如下：

a) 制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；

b) 事件发生后，应及时向信息系统的上级主管部门和同级的密码主管部门进行报告；

c) 事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。

附 录 A
（资料性附录）
安全要求对照表

表 A.1 不同安全保护等级的信息系统中密码技术应用要求

指标要求			一级	二级	三级	四级
技术要求	物理和环境安全	身份鉴别	可	宜	应	应
		电子门禁记录数据完整性	可	宜	应	应
		视频记录数据完整性	—	—	应	应
		密码模块实现	—	宜	宜	应
	网络和通信安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	宜	应	应
		通信数据完整性	可	宜	应	应
		通信数据机密性	可	宜	应	应
		集中管理通道安全	—	—	应	应
		密码模块实现	—	宜	宜	应
	设备和计算安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	宜	应	应
		敏感标记的完整性	可	宜	应	应
		日志记录完整性	可	宜	应	应
		远程管理身份鉴别信息机密性	—	宜	应	应
		重要程序或文件完整性	—	—	应	应
		密码模块实现	—	宜	宜	应
	应用和数据安全	身份鉴别	可	宜	应	应
		访问控制	可	宜	应	应
		数据传输安全	可	宜	应	应
		数据存储安全	可	宜	应	应
		日志记录完整性	可	宜	应	应
		重要应用程序的加载和卸载	—	—	应	应
		抗抵赖	—	—	—	应
		密码模块实现	—	宜	宜	应
密钥管理	生成		应	应	应	应
	存储		应	应	应	应
	使用		应	应	应	应
	分发		—	应	应	应
	导入与导出		—	应	应	应

表 A.1（续）

指标要求			一级	二级	三级	四级
密钥管理	备份与恢复		—	应	应	应
	归档		—	—	应	应
	销毁		—	—	应	应
安全管理	制度	制定密码安全管理制度	可	宜	应	应
		定期修订安全管理制度	可	宜	应	应
		明确管理制度发布流程	—	宜	应	应
		制度执行过程记录留存	—	—	—	应
	人员	了解并遵守密码相关法律法规	应	应	应	应
		正确使用密码相关产品	应	应	应	应
		建立岗位责任及人员培训制度	—	应	应	应
		建立关键岗位人员保密制度和调离制度	—	应	应	应
		设置密码管理和技术岗位并定期考核	—	—	应	应
		背景调查	—	—	—	应
	实施	规划	可	宜	应	应
		建设	可	宜	应	应
		运行	可	宜	应	应
	应急	应急预案	—	应	应	应
		事件处置	可	应	应	应
		向有关主管部门上报处置情况	—	—	应	应
注：“—”表示该项不做要求；“可”表示可以、允许；“宜”表示推荐、建议；“应”表示应该。						

附 录 B
（资料性附录）
密码行业标准列表

表 B.1 已发布密码行业标准列表

序号	标准编号	标准名称
1	GM/T 0001—2012	祖冲之序列密码算法
2	GM/T 0002—2012	SM4 分组密码算法
3	GM/T 0003—2012	SM2 椭圆曲线公钥密码算法
4	GM/T 0004—2012	SM3 密码杂凑算法
5	GM/T 0005—2012	随机性检测规范
6	GM/T 0006—2012	密码应用标识规范
7	GM/T 0008—2012	安全芯片密码检测准则
8	GM/T 0009—2012	SM2 密码算法使用规范
9	GM/T 0010—2012	SM2 密码算法加密签名消息语法规范
10	GM/T 0011—2012	可信计算 可信密码支撑平台功能与接口规范
11	GM/T 0012—2012	可信计算 可信密码模块接口规范
12	GM/T 0013—2012	可信计算 可信密码模块接口符合性测试规范
13	GM/T 0014—2012	数字证书认证系统密码协议规范
14	GM/T 0015—2012	基于 SM2 密码算法的数字证书格式规范
15	GM/T 0016—2012	智能密码钥匙密码应用接口规范
16	GM/T 0017—2012	智能密码钥匙密码应用接口数据格式规范
17	GM/T 0018—2012	密码设备应用接口规范
18	GM/T 0019—2012	通用密码服务接口规范
19	GM/T 0020—2012	证书应用综合服务接口规范
20	GM/T 0021—2012	动态口令密码应用技术规范
21	GM/T 0022—2014	IPSec VPN 技术规范
22	GM/T 0023—2014	IPSec VPN 网关产品规范
23	GM/T 0024—2014	SSL VPN 技术规范
24	GM/T 0025—2014	SSL VPN 网关产品规范
25	GM/T 0026—2014	安全认证网关产品规范
26	GM/T 0027—2014	智能密码钥匙技术规范
27	GM/T 0028—2014	密码模块安全技术要求
28	GM/T 0029—2014	签名验签服务器技术规范
29	GM/T 0030—2014	服务器密码机技术规范
30	GM/T 0031—2014	安全电子签章密码技术规范

表 B.1（续）

序号	标准编号	标准名称
31	GM/T 0032—2014	基于角色的授权与访问控制技术规范
32	GM/T 0033—2014	时间戳接口规范
33	GM/T 0034—2014	基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范
34	GM/T 0035—2014	射频识别系统密码应用技术要求
35	GM/T 0036—2014	采用非接触卡的门禁系统密码应用技术指南
36	GM/T 0037—2014	证书认证系统检测规范
37	GM/T 0038—2014	证书认证密钥管理系统检测规范
38	GM/T 0039—2015	密码模块安全检测要求
39	GM/T 0040—2015	射频识别标签模块密码检测准则
40	GM/T 0041—2015	智能 IC 卡密码检测规范
41	GM/T 0042—2015	三元对等密码安全协议测试规范
42	GM/T 0043—2015	数字证书互操作检测规范
43	GM/T 0044—2016	SM9 标识密码算法
44	GM/T 0045—2016	金融数据密码机技术规范
45	GM/T 0046—2016	金融数据密码机检测规范
46	GM/T 0047—2016	安全电子签章密码检测规范
47	GM/T 0048—2016	智能密码钥匙密码检测规范
48	GM/T 0049—2016	密码键盘密码检测规范
49	GM/T 0050—2016	密码设备管理 设备管理技术规范
50	GM/T 0051—2016	密码设备管理 对称密钥管理技术规范
51	GM/T 0052—2016	密码设备管理 VPN 设备监察管理规范
52	GM/T 0053—2016	密码设备管理 远程监控与合规性检验接口数据规范
53	GM/Z 4001—2013	密码术语
注：上表为截至 2017 年底已发布的密码行业标准，最新的密码行业标准列表信息请访问国家密码管理局网站，http://www.sca.gov.cn/。		

参 考 文 献

[1] 信息安全等级保护商用密码技术实施要求(2009 年白皮书)
[2] 商用密码应用安全性评估管理办法(试行)
[3] 信息安全技术 网络安全等级保护基本要求 第 1 部分:安全通用要求(2017 年征求意见稿)