# 6 密码安全管理方案

保障商用密码应用的合规性、正确性和有效性，不能仅靠技术，配套的管理也是必不可少的。根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，分别从管理制度、管理机构、建设运行、密钥管理、密码软硬件管理、人员管理和应急处置等几方面提出密码安全管理方案，建立配套密码安全管理制度，保障信息系统的正常运行以及数据安全，指导、规范信息系统密码应用的规划、建设、运行、应急及测评，为该系统提供管理方面的密码应用安全保障。

## 6.1 管理制度

依据《基本要求》《商用密码应用安全性评估管理办法（试行）》《信息系统密码测评要求（试行）》《商用密码应用安全性评估测评过程指南（试行）》《商用密码应用安全性评估测评作业指导书（试行）》等标准规范及管理要求为基础，结合ISO 270001(GB/T 22080)的体系的PDCA过程和ISO 27002（GB/T 22081）的14个控制域规范，同时兼顾监管部门的相关安全规范，整合企业自身的IT服务管理体系和技术安全控制体系，通过体系规范化、管理流程化、测量指标化、操作工具化等方式来确保管理体系设计的落地。密码安全管理制度体系主要包括：密码管理机构、密码建设、密钥管理、人员、设备等密码管理相关内容。此外同步在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规范内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

本管理办法适用于本单位密码设备、密钥、相关信息系统的管理、操作和维护活动。

本管理办法所称密码设备，包括但不限于服务器密码机签名验签服务器、智能密码钥匙等。

本管理办法所称密钥，包括但不限于非对称密钥对、对称密钥、MAC密钥等。

管理办法的执行机构是{{sysname}}。

## 6.2 管理机构

1. 本单位设立“{{sysname}}密码管理组织”，全面负责密钥生命周期、密码设备、设备证书的管理工作。
2. {{sysname}}密码管理组织至少由一名密钥管理员、一名密码安全审计员、一名密码操作员组成。
3. 所有的审批和操作指定专人负责，各类人员均应明确工作职责和管理权限，未经相关领导批准，不得擅自互换或代替。密码设备的管理账号、口令卡不得多人共用。
4. 密码管理负责人全面负责本单位密码管理的各项工作，统筹密码相关人员及工作安排，组织密码安全管理制度的制定及发布，负责密码相关人员考核等，组织开展定期或不定期的专项辅导检查工作。
5. 安全审计员负责监督审计本单位密码安全管理的各项工作，及时制止不正确操作，杜绝违规操作或越权操作行为。严格监督本单位密码相关重要岗位的工作状况，对不适合密码管理与维护工作或发现有不良行为的人员，提出调整建议。协助完成定期或不定期的专项辅导检查工作。
6. 密码设备管理员可由机房系统管理员兼任，负责维护密码设备正常运行，履行机房安全管理工作的一般性要求。协助完成定期或不定期的专项辅导检查工作。
7. 密钥操作员负责密钥的具体操作，完成密钥生成、备份、恢复、删除等操作过程。协助完成定期或不定期的专项辅导检查工作。
8. 密钥保管员负责密钥保管工作。接收密钥资料（组件），验证接收到的密钥资料是否受损；在监督下销毁密钥组件备份介质。协助完成定期或不定期的专项辅导检查工作。
9. 档案管理员负责收集、归档所有的审批和登记表格等密钥档案，按不同的操作特征和类型分类，保存在档案室、磁带备份室等安全区域；对档案建立较高的保密级别，未经书面授权，不允许借阅、复制及传播。维护经管理人 员授权后使用密钥的记录。协助完成定期或不定期的专项辅导检查工作。
10. 各类密码相关管理人员任用前，需签订保密协议，对本单位的密码设备配置、密钥、登录口令、敏感工作内容等均有保密义务。
11. 各类密码相关管理人员上岗前，需要参与必要的培训，包括熟悉密码相关管理制度，掌握各种密码设备的操作方法，明确相关工作流程规范等。
12. 各类密码相关管理人员每年应接受单位的考核，考核优秀者将给予奖励，考核不达标者要求重新参加培训，考核严重不合格者将调离本岗位。
13. 各类密码相关管理人员离职、退休或换岗前，需交回其管理的相关管理员介质、备份介质等密钥相关载体，密码管理负责人任命新任管理员后，把这些载体重新分配给新任管理员保管。新任密钥管理员上岗后，应及时召集其他密码管理员修改含有系统密钥的密码设备密码。

## 6.3 建设运行

系统的建设运行过程中，应注意的以下8点：

1. {{sysname}}，需要使用密码产品或密码模块时，应优先采购具有国家密码管理部门颁发的密码产品型号证书的密码产品或密码模块，若不能选购有资质密码产品，需要提供合理说明。
2. {{sysname}}，当需要使用密码服务时，应优先采购具有电子认证服务许可的电子认证机构的服务。
3. {{sysname}}，当需要使用密码算法时，应优先选择国家密码管理部门批准的密码算法，若不能采用国家密码管理部门批准的密码算法，需要提供合理说明。
4. 系统在规划阶段，应制定密码应用建设方案，并组织专家对建设方案进行评审，若系统已投入运行，需在系统改造前制定密码应用建设方案，组织专家对建设方案进行评审。
5. 系统在建设阶段，应制定密码应用实施方案，若系统已投入运行，需在系统改造过程中制定密码应用实施方案。
6. 信息系统投入运行前，应经商用密码应用安全性测评机构进行安全性评估，评估通过后方可投入正式运行，若系统已投入运行，改造后的系统应进行商用密码应用安全性评估。
7. 信息系统投入运行后，每年应委托商用密码应用安全性测评机构开展密码应用安全性评估，若系统已投入运行，改造后的系统应每年进行商用密码应用安全性评估。
8. 制定应急预案，定期开展应急演练，形成完善的安全事件处理和上报机制。

## 6.4 密钥管理

密钥管理主要分为7个步骤，具体如下：

1. 密钥的操作需由密钥应用方提出申请，由密码管理负责人签字确认，并制定密钥操作执行人，在密码设备管理员准备好硬件环境后，由密钥执行人进行操作。
2. 密码设备初始化由密码管理负责人和密钥操作员执行操作。具有口令卡的密码设备，管理员卡由密码管理负责人和密钥操作员分别持有。
3. 密钥的生成由密钥操作员执行操作。密钥在密码设备内由密码模块随机产生，密钥（除公钥外）不可以明文方式出现在密码模块之外。服务器密码机密钥生成后应马上进行密钥的备份操作。
4. 密钥的备份由密钥操作员执行操作，产生的备份卡、备份数据等由密钥保管员保管。
5. 密钥的恢复由密钥操作员执行操作，从密钥保管员处获取备份介质和数据。
6. 密钥的销毁应先进行密钥删除操作，再由密钥保管员对密钥备份卡、密钥备份文件进行物理销毁。
7. 上述各类密钥操作过程均应由安全审计员登记并保存记录。

## 6.5 密码软硬件管理

1. 密码设备应放置在严格安全管理措施的机房内，安装在带锁机柜中，机柜背板固定安装，对于密码设备的操作，配备摄像监控进行全过程监控，严禁打开密码设备机壳。
2. 在应用系统中禁止非法连接密码设备，新购买的密码设备应修改缺省口令，在密码设备报废时，应删除存储在该设备中的密钥。
3. 密码设备维修与升级要根据需求提出书面申请；密码设备生产厂商、维护商专人持有效身份证明文件，经证实获准。档案管理员详细记录工作日志，包括设备类型、故障现象、维修时间等要素。

## 6.6 人员管理

根据《基本要求》中密码安全管理人员方面的要求，{{sysname}}应制定相关的密码安全管理人员管理制度：

1. 设置内部密码专题培训机制，每6个月组织一次，由内部人员或聘请外部专家担任培训讲师，内容涉及密码相关法律法规和标准规范、商用密码应用、商用密码应用安全性评估等多个方面，使相关人员了解密码相关的法律和法规，掌握密码基本原理，并遵照执行。
2. 在密码应用系统建设完成后，安排项目建设单位、相关密码设备厂商对本系统部署使用的所有密码产品进行操作培训，确保相关人员能够正确配置使用本系统中部署的密码产品。
3. 结合{{sysname}}情况，分别设立密钥管理员、安全审计员、密码操作员等岗位，明确各岗位职责，对关键岗位建立多人共管机制，每个岗位均由2人担任；设备与系统的管理和使用账号不得多人共用。
4. 在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理人员、安全审计人员、密码操作人员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥管理人员、安全审计人员、密码操作人员与单位订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制度承担相应的保密义务。

## 6.7 应急方案

根据《基本要求》中安全管理应急方面的要求，{{sysname}}应制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施。主要包括：

1. 对信息系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施。
2. 当信息系统发生密码相关安全事件时，在事发后/事件处置完成后及时向用户主管单位进行报告。

### 6.7.1 潜在的安全事件分析

1. 事件分类

按项目时间周期划分，对系统可用性、安全性会造成影响的密码应用安全事件可以归纳为如下两类。

* 1. 项目实施过程中的安全事件

① 业务系统密码应用集成故障：因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统无法正常使用密码产品的事件。

② 密码产品部署故障：因密码产品实施人员工作疏忽，造成密码产品无法正常工作的事件。

③ 业务系统密码应用集成漏洞：因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统密码应用存在漏洞的事件。典型的有：身份鉴别时对证书有效性验证不严谨，造成已过期的、被注销的、非受信CA颁发的证书可以通过认证；身份鉴别时没有采用随机数签名，造成身份鉴别信息可被重放攻击等。

* 1. 密码运行过程中出现的安全事件

① **系统管理员证书失效：**系统管理员证书在过期前没有及时去续期、系统管理员证书介质PIN锁死或介质损坏的事件。这些会造成系统管理员无法正常登录业务系统进行维护和管理工作，对业务系统的可用性可能会造成影响。

② **业务系统服务器证书失效：**业务系统的服务器证书在过期前没有及时去续期、业务系统IP或域名修改的事件。这些会造成服务器证书验证失败，影响业务系统的正常访问。

③ **服务端密钥泄露：**主要是指服务端的服务器密码机、签名验签服务器设备里的密钥（包括私钥、对称密钥、MAC密钥）泄露事件。这些会造成关键敏感数据存储与传输的私密性、完整性被破解。

④ **服务端密码设备故障：**主要是指服务端的服务器密码机、签名验签服务器设备故障事件。这些会造成业务系统身份鉴别、数据安全存储、数据安全传输等功能异常。

⑤ **密码设备的安全漏洞：**主要是指服务器密码机、签名验签服务器、智能密码钥匙等密码设备存在软件或硬件上的安全漏洞事件。这些可能会造成密码设备可以被非法访问、私钥可被猜测等安全问题。

1. 事件定级

从以上的安全事件分类分析可知，不同的安全事件对系统可用性、安全性造成的破坏，严重程度不同。这里根据系统可用性和安全性遭受破坏的程度，对以上安全事件进行定级，分为一般事件、紧急事件、严重事件共三级。

* 1. 一般事件（I级）

一般事件只对系统可用性造成轻微破坏，稍加修正即可使系统恢复正常使用。一般事件不会影响到系统的安全性，主要包括：

① 业务系统密码应用集成故障

② 密码产品部署故障

③ 系统管理员证书失效

* 1. 紧急事件（II级）

紧急事件发生时能马上影响到系统可用性，且修复起来有一定的难度，但不会影响到系统的安全性，主要包括：

① 业务系统服务器证书失效

② 服务端密码设备故障

* 1. 严重事件（III级）

严重事件指能够影响到系统的安全性，主要包括：

① 业务系统密码应用集成漏洞

② 服务端密钥泄露

③ 密码设备的安全漏洞

### 6.7.2 应急处置组织机构与职责

1. 密码服务组织机构

{{sysname}}应结合其日常组织机构建立密码服务应急响应的组织机构，并明确其职责。其中一些人可负责两种或多种职责，一些职位可由多人担任（应急响应计划文档中应明确他们的替代顺序）。

应急响应的组织机构由管理、业务、技术和行政后勤等人员组成，一般可设为应急响应领导小组、应急响应实施小组和应急响应日常运行小组等。组织可聘请具有相应资质的外部专家协助应急响应工作，也可委托具有相应资质的外部机构承担实施小组以及日常运行小组的部分或全部工作。在聘请外部专家协助应急响应工作或者委托外部机构承担部分或者全部应急工作时需要和其签订相关协议（例如签订有关信息保密要求等）。

1. 应急响应领导小组

{{sysname}}应组建应急响应领导小组，应急响应领导小组是信息安全应急响应工作的组织领导机构，组长应由组织最高管理层成员担任。领导小组的职责是领导和决策信息安全应急响应的重大事宜，主要如下：

* 1. 审核并批准经费预算
  2. 审核并批准恢复策略
  3. 审核并批准应急响应计划
  4. 批准应急响应计划的执行

1. 应急响应日常运行小组

应急响应日常运行小组的主要职责是：

* 1. 协助恢复密码服务的实施
  2. 备份中心密钥管理
  3. 管理信息系统的运行的密码服务设备
  4. 密码服务灾难恢复的专业技术支持
  5. 参与和协助密码服务应急响应计划的教育、培训和演练
  6. 维护和管理应急响应商用密码服务计划文档
  7. 密码服务突发中止事件发生时的损失控制和损害评估
  8. 密码服务中止发生后的恢复
  9. 密码服务中止发生后的外部协作

1. 应急响应厂商

应急响应厂商的主要职责是：

* 1. 协助恢复密码服务的实施
  2. 密码服务的专业技术支持
  3. 参与和协助商用密码服务应急响应计划的教育、培训和演练
  4. 密码服务中止发生后的恢复

### 6.7.3 应急处置预案设计

针对潜在的安全事件，进行了应急处置预案的设计。

1. 项目实施过程中的安全事件应急处置预案

针对项目实施过程中的安全事件，应急处置预案设计如下，包括系统密码应用集成故障、密码产品部署故、密码应用集成漏洞。

* 1. 系统密码应用集成故障，如表 6.1所示。

表6.1 系统密码应用集成故障

|  |  |
| --- | --- |
| 出现问题的原因 | 因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统无法正常使用密码产品的事件。 |
| **问题影响** | 密码应用在业务的生产系统验证失效 |
| **事前防范** | 上线生产前做多次模拟生产运行的验证测试 |
| **事中处理** | 进行密码应用算法回退；  进行数据恢复。 |
| **事后处置** | 校验模拟系统和生产系统间的差异；  充份分析所遇到的问题细节；  待所有问题解决后再进行二次上线验证。 |
| **损失评估** | 延误了系统密码算法安全性整体更新的进度 |

* 1. 密码产品部署故障，如表 6.2所示。

表 6.2 密码产品部署故障

|  |  |
| --- | --- |
| 出现问题的原因 | 因密码产品实施人员工作疏忽，造成密码产品无法正常工作的事件。 |
| **问题影响** | 上线生产后密码产品设备不工作或工作异常 |
| **事前防范** | 上线生产前充份验证设备配置文档，并且多次做模拟生产上运行环境的压力测试和功能测试 |
| **事中处理** | 进行密码应用算法回退；  密码产品部署回退，定位问题。 |
| **事后处置** | 分析模拟系统和生产系统间的差异；  全面分析失败上线的原因；  待所有问题解决后再进行二次上线，验证。 |
| **损失评估** | 延误了系统密码算法安全性整体更新的进度 |

* 1. 密码应用集成漏洞，如表 6.3所示。

表 6.3 密码应用集成漏洞

|  |  |
| --- | --- |
| 出现问题的原因 | 因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统密码应用存在漏洞的事件，典型的有：身份鉴别时对证书有效性验证不严谨，造成已过期的、被注销的、非受信CA颁发的证书可以通过认证；身份鉴别时没有采用随机数签名，造成身份鉴别信息可被重放攻击等 |
| **问题影响** | 有心攻击信息的黑客很容易蒙混到信息系统内部，引发内部信息泄漏风险 |
| **事前防范** | 技术上对认证的原理进行了理论性的认证，并给出了集成的拓扑说明；  可复制参考的集成示例，接口介绍文档；  宽且广的测试案例的覆盖。 |
| **事中处理** | 系统全面回退到使用证书登录前的状态；  待所有问题解决后再进行二次上线，验证。 |
| **事后处置** | 开发人员重新参考方案，做原理层的深入了解，充分理解示例代码，接口说明文档；  重新做证书认证产品的接入；  宽且广的测试案例的覆盖，β测试。 |
| **损失评估** | 延误了强身份认证的上线进度，给系统安全性存在身份认证方面的不足，容易受到黑客密码穷举，撞库等方面的攻击，存在内部信息泄漏的风险。 |

1. 密码运行过程中出现的安全事件应急处置预案

针对密码运行过程中的安全事件，应急处置预案设计如下，包括系统管理员证书失效、系统服务器证书失效、密钥泄漏、密码设备故障、密码设备的安全漏洞。

* 1. 系统管理员证书失效，如表 6.4所示。

表 6.4 系统管理员证书失效

|  |  |
| --- | --- |
| 出现问题的原因 | 系统管理员证书在过期前没有及时去续期、系统管理员证书介质PIN锁死或介质损坏。 |
| **问题影响** | 系统管理员无法正常登录业务系统进行维护和管理工作，对业务系统的可用性可能会造成影响。 |
| **事前防范** | 设立规范制度要求：管理员每个月定期查看系统管理员证书的有效时间，设置两个管理证书介质互为备份。 |
| **事中处理** | 采用备份的管理证书介质登录系统；  使用备份的管理员介质做常用的系统管理员的新证书。 |
| **事后处置** | 加强规范制度的落实措施；  强调备份的重要性，备份的使用周期要比应用中的产品周期长1.5-2倍。 |
| **损失评估** | 管理员登录不及时导致系统维护不及时，造成密码服务的连续性服务中断。 |

* 1. 系统服务器证书失效，如表 5.6所示。

表 6.5 系统服务器证书失效

|  |  |
| --- | --- |
| 出现问题的原因 | 业务系统的服务器证书在过期前没有及时去续期；业务系统IP或域名修改没有及时申请新的IP或域名证书。 |
| **问题影响** | 服务器证书验证失败，影响业务系统的正常访问 |
| **事前防范** | 设立规范制度要求管理员每个月定期查看服务器的有效时间，确定服务器证书可继续服务的时间。  系统的任意修改需要做出风险评估后，落实准备条件再做切换或更改。 |
| **事中处理** | 针对证书过期问题，一方面管理员需要尽快为过期的服务器证书续期；另一方面向CA机构申请临时服务器证书过渡网站正常应用。  没有及时申请新问题，采用IP或域名回退机制，待新证书申请下来后再做IP或域名的切换。 |
| **事后处置** | 加强规范制度的落实措施；  加强从测试到生产的验证性测试。 |
| **损失评估** | 影响信息系统的IP或域名切换进度，临时证书申请过程和机制回退造成密码服务的连续性服务中断。 |

* 1. 密钥泄漏，如表 6.6所示。

表 6.6 密钥泄漏

|  |  |
| --- | --- |
| 出现问题的原因 | 服务端的服务器密码机、签名验签服务器设备里的密钥（包括私钥、对称密钥、MAC密钥）泄漏事件。 |
| **问题影响** | 关键敏感数据存储与传输的私密性、完整性被破解 |
| **事前防范** | 密钥对应的信息系统应用模块做好登记；  多套密钥同时运行。 |
| **事中处理** | 评估密钥泄漏可能波及到的系统范围；  在密码服务系统中采用新的一套密钥；  信息系统尽快做好密钥切换工作与新密钥验证；  销毁旧密钥，做好新密钥的备份措施和安全控制措施。 |
| **事后处置** | 追踪密钥外泄的原因；  加强制度的管理；  强化密钥管理安的全意识。 |
| **损失评估** | 密钥外泄的信息系统数据存在泄漏的风险 |

* 1. 密码设备故障，如表 6.7所示。

表 6.7 密码设备故障

|  |  |
| --- | --- |
| 出现问题的原因 | 服务端的服务器密码机、签名验签服务器设备故障事件。 |
| **问题影响** | 业务系统身份鉴别、数据安全存储、数据安全传输等功能异常 |
| **事前防范** | 做好密码服务设备的双套运行备份；  做好密码服务设备的密钥备份。 |
| **事中处理** | 马上使用备用设备替换现有密码服务系统设备，隔离出问题的密码服务系统设备。  分析出问题的设备的原因，做好必要记录，妥善保存有关记录及日志或审计记录。  如果满足下列情况之一的，应立即向信息中心负责人通报情况，申请由应急响应小组协助处理：  密码服务系统设备在2小时内无法处理完毕的。  密码服务系统设备涉临淘汰，市场上无法找到替代密码服务的设备。  在应急响应小组协助修复设备后，进行密码系统和相关数据恢复，检查密码系统数据的完整性。  相关密码服务故障事件处理完毕，重新接入网络。 |
| **事后处置** | 总结事件处理情况，将有关情况向安全领导小组领导汇报有关情况，并提出防范再度爆发的解决方案。  配合应急响应小组实施必要的安全加固。 |
| **损失评估** | 主备机的切换影响密码连续性工作的中断 |

* 1. 密码设备的安全漏洞，如表 6.8所示。

表 6.8 密码设备的安全漏洞

|  |  |
| --- | --- |
| 出现问题的原因 | 服务器密码机、签名验签服务器、智能密码钥匙等密码设备存在软件或硬件上的安全漏洞事件。 |
| **问题影响** | 密码设备可以被非法访问、私钥可被猜测等安全问题 |
| **事前防范** | 及时根据密码服务设备厂家发布的漏洞进行补丁修复；  定期观查密码服务器的运行日志，把握密码设备的运行状态。 |
| **事中处理** | 及时根据密码服务设备厂家发布的漏洞进行补丁修复。 |
| **事后处置** | 加强与密码设备厂家的沟通，尽可能在漏洞公布后及时进行补丁修复；  评估漏洞事件可能带来的系统风险。 |
| **损失评估** | 密码设备可以被非法访问、私钥可被猜测等安全问题可能会导致用户数据外泄，安全数据泄漏的风险。 |