# 6 安全管理方案

**参照GB/T22240中等级保护定级,根据GB/T39786对该等级的管理要求,根据部署的密码产品管理机制,设计安全管理方案,包括管理制度、人员管理、建设运行和应急处置方面的制度。示例写法如下：**

## 6.1管理制度

保障商用密码应用的合规性、正确性和有效性，除了技术，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》，分别从密码安全管理制度、人员管理、密钥管理、建设运行、密码软硬件及介质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。

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。

## 6.1 密码安全管理制度

为了加强密码设备管理工作，确保安全使用密码，根据《中华人民共和国密码法》、《商用密码管理条例》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等国家有关法规规定，制定本制度。单位涉及密码管理、使用和运维等相关人员均需遵守本规定。

### 6.1.1 密码建设要求

1、信息系统密码建设应符合密码相关法律与行业相关政策要求进行建设。

2、统筹系统密码应用，应与业务系统统一设计，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

3、信息系统规划阶段，依据相关标准，制定密码引用方案，组织专家进行评审，评审意见作为项目规划立项重要材料。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。

4、对未及时开展密码建设的系统，应逐步完成密码建设的备案、整改、测评等工作。

5、密码建设产品应当采用符合国家密码管理部门核准的密码产品、许可的密码服务，产品应具备最新商用密码产品型号证书的产品。

### 6.1.2 密码运行要求

1、信息系统投入运行前，应经过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。

2、信息系统投入运行后，本单位主管责任人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；如若有重大安全隐患，应停止系统运行，制定整改方案，整改完成并通过后方可投入运行。

### 6.1.3 密码人员管理要求

1、结合系统分析、风险分析和安全需求分析的结果，明确密码安全管理人员。

2、结合系统建设具体现状明确本管理机构内密码管理人员组成与职能，明确管理责任，做到责任到部门、责任到人。

3、根据密码管理政策、数据安全保密政策，结合本组织实际情况，设立密钥管理员、密码安全审计员、密码操作员等关键安全岗位。

4、密钥管理员、密码安全审计员、密码操作员人员职责相互制约相互监督，关键设备的管理和使用账号不得多人共用。

5、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。

6、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。

7、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。

### 6.1.4 密码使用责任要求

1、密码使用单位应当建立密码管理责任人，落实信息系统密码应用工作。

2、密码使用单位应严格遵循相关要求，使用密码技术完善系统的安全保护功能，因密码使用不当导致信息泄密、数据破坏的，追究相关单位密码管理部门和管理人员责任，并按要求整改。

3、本单位应当严格遵守相关保密制度，保管好个人数字证书，不得出借或使用他人证书登录信息系统平台。

4、个人数字证书介质一旦丢失，应立即进行挂失，并按规定流程到证书发放机构申请新的证书和介质。

### 6.1.5 密码设备维护规定

1、密码设备维护人员需经过培训，取得相关资质才能上岗，并需严格按照设备维护规范和使用说明开展维护工作。

2、密码设备应当按照要求定期完成设备巡检、升级和维保工作，至少每半年集中检查一次，密码设备操作必须经过授权，且不得接入互联网访问。

3、建立密码设备故障和应急保障机制，定期开展应急演练，确保设备发生故障时能及时上报、恢复。事件处理完成后及时向同级密码负责人报告事件发生情况和处理办法。

4、加强密码设备的日常监控，评估系统安全风险，及时进行扩容和升级。

## 6.2 人员管理

依据本单位《商用密码安全管理制度》设立本管理制度，主要用于对人员的相关合规性要求、培训、奖惩制度的说明和建立。

### 6.2.1 总章

密码人员应了解并遵守密码相关法律法规。

在岗密码人员应能够正确、合理使用密码产品。

### 6.2.2 第一章 密码人员岗位与职责

1、结合系统分析、风险分析和安全需求分析的结果，明确密码安全管理人员。

2、结合系统建设具体现状明确本管理机构内密码管理人员组成与职能，明确管理责任，做到责任到部门、责任到人。

3、根据密码管理政策、数据安全保密政策，结合本组织实际情况，设立密钥管理员、密码安全审计员、密码操作员等关键安全岗位，并制定规范边界任务。

#### 密码系统管理员职责

制定严格的规章制度并认真执行。建立完善的变更管理审核和批准制度，对任何可能影响系统正常运行的密码软硬件变更，包括更改设置、软硬件升级等，应及时登记报备。

#### 密钥管理员职责

负责对应用系统密钥的保管、监督、变更、撤销等具体操作，包括对密钥的生成、存储、分发、导入导出、使用、备份恢复、归档、销毁等全生命周期的管理。协助完成定期或不定期的专项辅导检查工作。

#### 密码安全审计员职责

密码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。

#### 密码操作员职责

认真执行密码安全相关制度；管理用户账户的密码，包括密码重置、设置和解锁；遵循密码策略，确保用户密码的复杂性和安全性；记录密码变更和重置的审计日志。协助完成定期或不定期的专项辅导检查工作。

### 6.2.3 第二章 密码人员培训规范

1、制定密码人员学习管理制度。制定密码人员学习、培训档案管理、培训考核等相关制度要求。

2、培训参加。定期参与省密码管理局开展的密码培训会议，使密码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。建立本单位内密码培训工作档案，记录包括培训范围、培训方式、培训内容、培训人数、培训时间和其他情况。

3、人员档案管理。建立针对密码管理人员建立员工培训档案，接收培训的具体情况和培训结果应详细记录备案，包括培训时间、培训地点、培训内容、培训目的以及培训效果。

4、培训档案管理。应对培训过程进行记录保存，培训资料应以纸质、电子文档、录音、录像等形式记录保存，并通过口令或专用加密软件加密保存至专用存储设备（如U盘、移动硬盘、NAS服务器等，纸质应单独文件柜）统一管理，培训档案留存时间应保存五年，五年后可销毁。

5、日常工作应用。针对密码人员的日常工作进行评估，针对培训填写“课程评估调查表”对省密码管理局是否具备工作改善计划或方案。

### 6.2.4 第三章 密码人员考核与奖惩

1、依托本单位人员绩效考核管理制度，制定密码人员考核管理办法。

2、针对测评机构、市密码管理局、省密码管理局、国家密码管理局的定期检查、抽查效果作为基本考核单元。对重大隐患、系统测评问题应及时上报处理、备案。

3、定期针对业务系统开展密码使用情况年度自查，并纳入责任单位相关人员考核。

4、在当年密码应用考核中被处理的，原则上取消当年评优评先资格。

5、在当年密码应用考核中表现突出的，依托本单位人员绩效考核管理制度酌情予以表彰、评优评先。

## 6.3 密钥管理

本单位依据《商用密码安全管理制度》设定对密钥管理的相关管理制度。管理内容包括对密钥的生成、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。

### 6.3.1 密钥生成

本单位所使用的密钥生成使用的随机数均符合GM/T 0005要求，密钥均在符合GM/T 0028的密码模块中产生；密钥均在密码模块内部产生，不会以明文方式出现在密码模块之外；密码模块均具备检查和剔除弱密钥的能力。

### 6.3.2 密钥存储

本单位所使用的密钥均采用加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥均存储在符合GM/T 0028的二级及以上密码模块中。

### 6.3.3 密钥分发

本单位在密钥分发时均采取身份鉴别、数据完整性、数据机密性等安全措施，均能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

### 6.3.4 密钥导入与导出

本单位已采取安全措施，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。

### 6.3.5 密钥使用

本单位在密钥使用时已明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前均对其进行验证；均有安全措施防止密钥的泄露和替换；密钥泄露时，立即停止使用，并启动相应的应急处理和响应措施。密钥使用时均按照密钥更换周期要求更换密钥；已采取有效的安全措施，保证密钥更换时的安全性。

### 6.3.6 密钥备份与恢复

本单位已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，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。

### 6.3.7 密钥归档

本单位已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。

### 6.3.8 密钥销毁

本单位已具有在紧急情况下销毁密钥的措施。

## 6.4 建设运行

系统的建设运行过程中，应注意的以下8点：

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。

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。

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。

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。

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。

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。

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。

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。

## 6.5 密码软硬件及介质管理

认真执行岗位责任制和相关规章制度。

严格遵守安全操作规程，保证密码设备的安全运行。

及时准确地填写各项原始记录和统计报表，并及时反馈密码设备存在的问题。

密码设备操作人员必须经过培训，并留存培训记录。

密码设备操作应由密码操作人员进行，禁止任何非专业人员对机房设备进行任何操作。

密码设备操作应严格遵守相关规章制度和操作规范。

密码设备操作应由两人或两人以上互相监督操作运行，确保操作正确。

密码设备操作前应检查，操作后应查看策略，确保业务能够正常运行。

对于可能影响业务的操作，操作前需要提前进行测试，或在专业人员配合下操作，确保安全后方可执行。

严禁在各密码设备或管理客户端上安装一切与操作无关的软件。

严禁将来历不明的移动存储介质（含光盘、磁盘、优盘等）在密码设备、管理客户端上使用。

操作时若需要连接笔记本电脑操作，应制定操作密码专用笔记本进行操作，专用笔记本应由专人保管，并设置复杂度较高的口令，由操作人员进行管理。设备应严禁安装与操作无关的任何软件等。操作专用笔记本禁止连接外网；专用笔记本电脑应当安装防病毒软件并定期更新，更新时应使用优盘通过补丁进行更新，确保系统安全。

厂家人员操作，应用相关技术人员全程陪同监督。

若需要远程操作，应由相关人员提出申请，经审批后方可执行。厂家人员远程操作，应确保两人及以上同时进行远程操作，同时由相关技术人员陪同并得到证实。

在申请数字证书时应提供真实、完整、准确的身份信息和其他相关信息，并在这些信息变更时及时到与密码小组管理员沟通变更手续；

获取数字证书时，应当使用安全的工具产生并存储私钥及证书，比如使用USB Key来存储数字证书；使用完USB Key后应立即将其从电脑上拔出，不要将USB Key长时间留在电脑上；不使用已被证实产生弱私钥的工具来产生私钥。

设置密码口令时，避免设置与个人资料相关的简单口令，如身份证号码、出生日期、电话号码等，应定期更改口令；

务必妥善保管数字证书使用密码口令及存储数字证书的USB Key设备，防止机密信息泄漏或被他人窃取；如果数字证书遗失，或者发现相关的密码泄漏，务必及时到申请网点办理挂失手续并按照规定重新办理证书和/或设置密码；

避免在公共场所或他人计算机上使用数字证书；

在使用数字证书的电脑上要及时安装操作系统和浏览器的最新安全补丁，提高系统安全性；安装个人防火墙，防止他人的非法访问和恶意攻击；安装并定期更新防病毒软件，防止受到新病毒的侵害；切勿在使用数字证书的电脑上随意登陆不明网络站点，下载、安装不明软件或运行不明程序。

## 6.6 应急方案

根据《基本要求》中安全管理应急方面的要求，系统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。

### 6.6.1 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。

（2） 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。

2、 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

（2） 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

（3） 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

### 6.6.2 应急处置组织机构与职责

1、密码服务组织机构

系统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）。

2、应急响应领导小组

系统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

3、 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

4、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

### 6.6.3 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；  充分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** | 有心攻击信息系统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。 |

2、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。 |

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。  没有及时申请新的IP或域名证书，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。 |

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机密性、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；  定期查看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。 |