



中华人民共和国密码行业标准

GM/T 0132—2023

信息系统密码应用实施指南

Implementation guide for information system cryptography application

2023-12-04 发布

2024-06-01 实施

国家密码管理局 发布

目 次

前言.....Ⅲ

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 信息系统密码应用实施概述.....1

 4.1 角色和职责.....1

 4.2 基本流程.....2

5 信息系统密码应用规划.....2

 5.1 规划阶段的工作流程.....2

 5.2 密码应用需求分析.....3

 5.2.1 信息系统现状分析.....3

 5.2.2 密码应用安全风险分析.....4

 5.2.3 密码应用基本需求的确定.....4

 5.2.4 密码应用特殊需求的确定.....4

 5.2.5 需求分析结果文档化.....5

 5.3 密码应用方案设计.....5

 5.3.1 总体策略设计.....5

 5.3.2 密码应用技术方案设计.....5

 5.3.3 密码应用安全管理方案设计.....6

 5.3.4 合规性自查.....6

 5.3.5 实施保障方案设计.....6

 5.3.6 设计结果文档化.....7

 5.4 方案密评.....7

6 信息系统密码应用建设.....8

 6.1 建设阶段的工作流程.....8

 6.2 密码建设方案设计.....8

 6.2.1 密码应用技术措施实现内容的设计.....8

 6.2.2 密码应用安全管理措施实现内容的设计.....9

 6.2.3 设计结果文档化.....9

 6.3 密码应用技术措施的实现.....9

 6.3.1 密码产品与密码服务采购.....9

 6.3.2 密码应用集成.....10

6.4 密码应用安全管理措施的实现.....10

6.4.1 密码应用配套安全管理制度的制定.....10

6.4.2 密码管理岗位和人员的设置.....10

6.4.3 建设过程管理.....11

6.5 系统密评.....11

7 信息系统密码应用运行.....12

7.1 运行阶段的工作流程.....12

7.2 运行管理和控制.....13

7.2.1 运行管理过程控制.....13

7.2.2 运行管理人员控制.....13

7.3 变更管理和控制.....13

7.3.1 变更需求和影响分析.....13

7.3.2 变更过程控制.....14

7.4 密码应用安全状态监控.....14

7.4.1 监控对象确定.....14

7.4.2 监控对象状态信息收集.....14

7.4.3 监控状态分析和报告.....15

7.5 安全自查和持续改进.....15

7.5.1 密码应用安全状态自查.....15

7.5.2 密码应用整改.....16

7.6 系统密评.....16

7.7 应急响应与保障.....17

7.7.1 应急准备.....17

7.7.2 应急监测与响应.....17

7.7.3 后期评估与改进.....18

7.7.4 应急保障.....18

8 信息系统密码应用终止.....18

8.1 终止阶段工作流程.....18

8.2 密码应用信息转移、暂存和清除.....19

8.3 密码应用设备迁移或废弃.....19

8.4 密码应用存储介质的清除或销毁.....20

附录 A（规范性） 主要过程及其活动和输入输出.....21

参考文献.....24

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：兴唐通信科技有限公司、国家密码管理局商用密码检测中心、中国科学院信息工程研究所、中国科学院数据与通信保护研究教育中心、北京信安世纪科技有限公司、北京数盾信息科技有限公司、三未信安科技股份有限公司、阿里云计算有限公司、中电科网络安全科技股份有限公司、公安部第三研究所、蚂蚁科技集团股份有限公司、鼎铉商用密码测评技术(深圳)有限公司、北京天融信网络安全技术有限公司、中金金融认证中心有限公司、阿里巴巴(中国)网络技术有限公司、上海市数字证书认证中心有限公司、中互金认证有限公司、国家信息技术安全研究中心、深圳市腾讯计算机系统有限公司、中国电子科技集团公司第十五研究所、中国国家铁路集团有限公司、暨南大学、启明星辰信息安全技术有限公司。

本文件主要起草人：王彦力、刘尚焱、许长伟、王兵、马原、郑昉昱、肖秋林、吴星宇、贾世杰、田爱军、孙丽伟、姚长远、胡伟、何济尘、梅秋丽、汪宗斌、秦体红、吴冬宇、刘健、张立花、杨辰、陈天宇、吕娜、袁静、乐宏彦、陈萧宇、许涛、张大江、周君平、张宇翔、宋铮、陈磊、万志宇、马春旺、朱红儒、谭武征、李增局、姬生利、杨龙、田涛、于航、高志权、鹿淑煜、吴波、华珊、李升、方海峰、肖飞、安高峰、贺磊、司华峰、彭晋、黄天宇、李冰、谢旭、蒋增增、苏继海、孙欣、刘志刚、史汝辉、朱凌。

信息系统密码应用实施指南

1 范围

本文件给出了信息系统密码应用的流程指导和建议,描述了规划、建设、运行及终止阶段的实施过程及主要活动。

本文件适用于指导信息系统密码应用的实施。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 20984	信息安全技术 信息安全风险评估方法
GB/T 39786	信息安全技术 信息系统密码应用基本要求
GM/T 0115	信息系统密码应用测评要求
GM/T 0116	信息系统密码应用测评过程指南
GM/Z 4001	密码术语

3 术语和定义

GB/T 39786 和 GM/Z 4001 界定的术语和定义适用于本文件。

4 信息系统密码应用实施概述

4.1 角色和职责

信息系统密码应用中涉及的各类角色及其职责如下。

- a) 密码管理部门
负责依法管理密码工作。
- b) 信息系统责任单位

通常包括项目建设单位以及信息系统运营、使用单位,负责依照信息系统密码应用的管理规范和技术标准,进行密码应用方案的设计;使用符合国家规定、满足信息系统对应等级密码应用基本要求的密码算法、密码技术、密码产品和密码服务,开展信息系统密码应用建设或整改工作;制定、落实各项密码应用配套安全管理制度,定期对信息系统密码应用安全状况、密码应用配套安全管理制度及措施的落实情况进行自查;自行或委托商用密码应用安全性评估机构开展商用密码应用安全性评估(简称“密评”),包括密码应用方案密评(简称“方案密评”)和信息系统密评(简称“系统密评”);对密码应用安全事件进行应急处置。

- c) 密码应用集成服务单位

负责根据信息系统责任单位的委托,依照信息系统密码应用的管理规范和技术标准,协助信息系统责任单位完成信息系统密码应用的规划、建设、运行及终止阶段的工作(包括但不限于密码应用咨

询、密码应用需求分析、密码应用方案设计、密码应用集成建设或整改服务)。

d) 商用密码应用安全性评估机构

负责按照标准(包括但不限于 GB/T 39786、GM/T 0115 和 GM/T 0116)和指导文件,对密码应用方案或信息系统开展密评。商用密码应用安全性评估机构简称“密评机构”。

e) 密码产品和服务提供单位

负责依照信息系统密码应用的管理规范和技术标准,开发和提供密码产品或密码服务。

4.2 基本流程

信息系统密码应用的实施流程包括规划、建设、运行和终止四个阶段,基本流程见图 1。

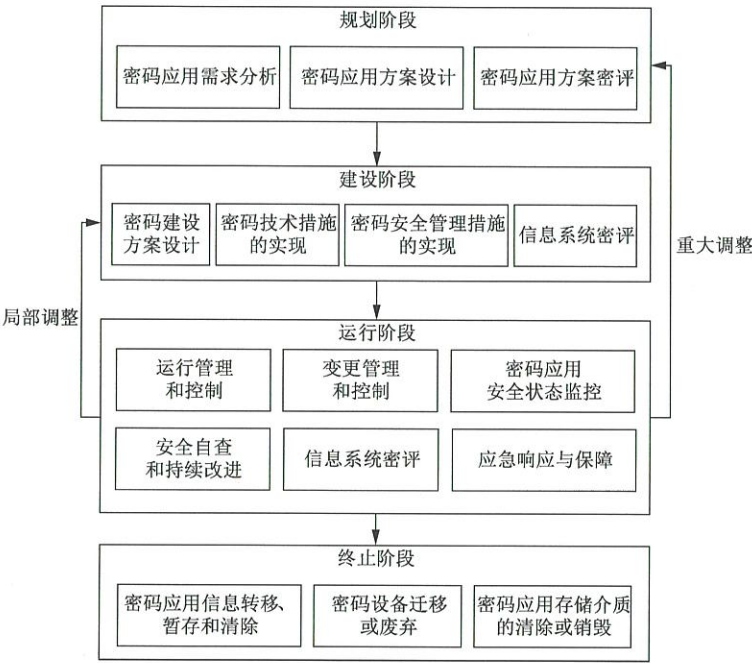


图 1 信息系统密码应用实施基本流程

系统密评在密码应用运行期间遵循持续改进的原则是十分必要的。信息系统因需求变化、未通过密评导致局部调整,将从运行阶段进入建设阶段,根据问题进行整改,确保满足信息系统密码应用的要求。当信息系统发生重要变化(如部署位置、系统结构、主要软件与硬件组成、主要密码产品等发生重大变化可能带来高风险问题)、信息系统密码应用安全要求等级发生变化、重大密码相关安全事件导致重大调整,需要修改密码应用方案时,将从运行阶段进入规划阶段,重新开始信息系统密码应用的实施过程。

对于未制定密码应用方案的信息系统,无论信息系统是否已开工建设、上线运行,其密码应用的建设或改造过程均视为从规划阶段开始。

信息系统密码应用实施的基本流程中各个阶段的主要过程、活动、输入和输出按照附录 A 的规定。

5 信息系统密码应用规划

5.1 规划阶段的工作流程

信息系统密码应用规划阶段的目标是根据信息系统的基本情况、网络拓扑、软件与硬件组成、承载

业务情况信息、安全需求情况,按照 GB/T 39786 的要求,分析并明确信息系统的密码应用需求,设计明确的密码应用方案。信息系统密码应用规划阶段的工作流程见图 2。

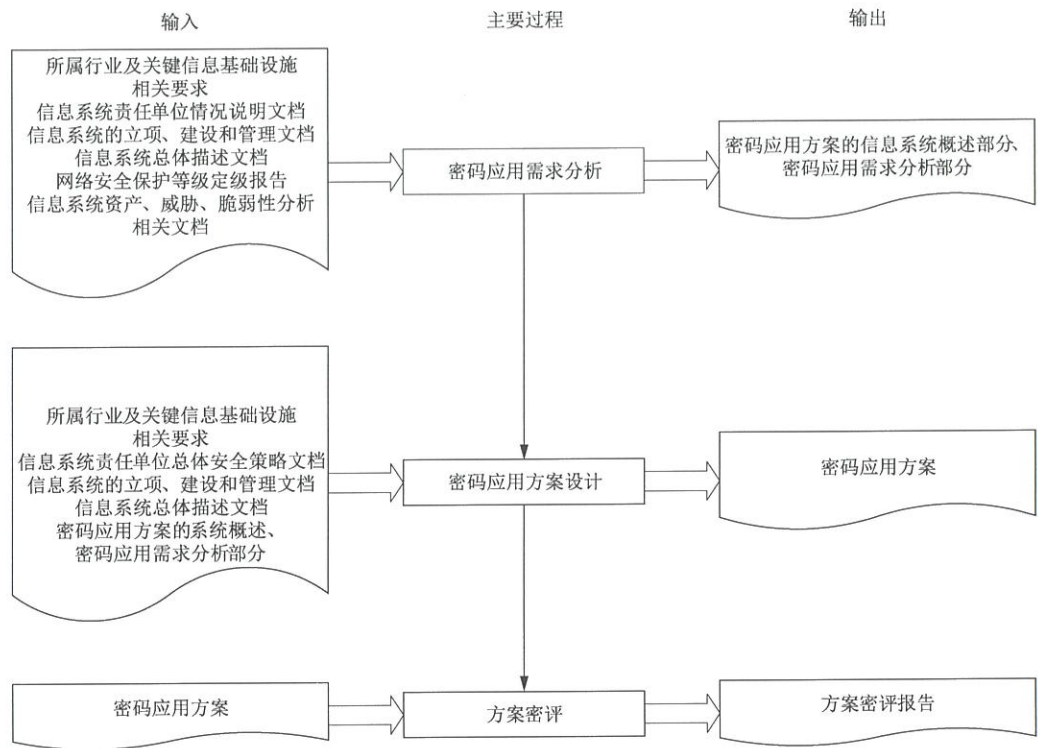


图 2 信息系统密码应用规划阶段的工作流程

5.2 密码应用需求分析

5.2.1 信息系统现状分析

活动目标：

通过收集了解信息系统情况,并进行综合分析和整理,形成信息系统现状的综合情况描述。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:单位情况说明文档,信息系统的立项、建设和管理文档,信息系统总体描述文档,网络安全保护等级定级报告。

活动描述：

本活动主要包括以下子活动内容。

a) 识别信息系统总体信息

了解信息系统的总体信息,包括基本情况、网络拓扑、承载的业务情况、软件与硬件组成。

b) 识别信息系统的管理情况

了解信息系统的管理情况,包括管理机构、管理人员、管理职责、管理制度、安全策略。

c) 识别信息系统的信息资产

调查信息系统处理的信息资产,根据数据分类分级国家和行业标准规范,识别需要保护的重要信息资源和重要数据。

d) 确定信息系统密码应用安全要求等级

根据信息系统的网络安全保护等级,确定信息系统密码应用安全要求等级。

若信息系统未完成网络安全等级保护定级,则根据拟定级情况确定信息系统密码应用安全要求等级。

e) 信息系统综合描述

对收集的信息进行整理、分析,从以下方面形成对信息系统现状的描述:

- 1) 信息系统基本情况;
- 2) 信息系统网络拓扑;
- 3) 信息系统承载的业务情况;
- 4) 信息系统软硬件构成;
- 5) 信息系统管理情况;
- 6) 需要保护的重要信息资产,包括但不限于重要信息资源、重要数据;
- 7) 信息系统密码应用安全要求等级。

活动输出:密码应用方案的信息系统概述部分。

5.2.2 密码应用安全风险分析

活动目标:

根据信息系统现状,分析信息系统中存在的密码应用安全风险。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:信息系统总体描述文档,网络安全保护等级定级报告,信息系统资产、威胁、脆弱性分析文档。

活动描述:

按照 GB/T 39786 相应级别的指标要求,逐条分析信息系统目前现状对指标要求的满足情况,针对不满足指标要求的,按照 GB/T 20984 分析其面临的安全风险。

活动输出:密码应用方案的安全风险分析部分。

5.2.3 密码应用基本需求的确定

活动目标:

根据信息系统密码应用的安全风险分析,提出信息系统密码应用的基本需求。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案的安全风险分析部分。

活动描述:

按照 GB/T 39786 中相应等级的指标要求,从物理和环境安全、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技术基本需求,确定各个层面中不涉及相应密码应用需求的指标项,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密码应用管理基本需求。其中,在网络和通信安全层面,需要特别关注连接不同信息系统的通信信道的责任方归属问题,明确相应通信信道的密码应用要求;在应用和数据安全层面,需要重点明确信息系统用户不同登录方式的真实性保护需求,明确每一类重要数据的完整性或机密性保护需求,明确信息系统业务活动中的不可否认性保护需求。

活动输出:密码应用方案的密码应用基本需求部分。

5.2.4 密码应用特殊需求的确定

活动目标:

根据信息系统的行业特点、关键信息基础设施和重要数据的特殊保护要求,提出信息系统的密码

应用特殊需求。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案的安全风险分析部分、所属行业及关键信息基础设施相关要求。

活动描述:

本活动主要包括以下子活动内容。

a) 合规性特殊需求

针对信息系统面临的实际安全风险,遵照所属行业及关键信息基础设施和重要数据相关的法律法规和要求、主管部门提出的密码应用要求,以及关键信息基础设施标准中提出的 GB/T 39786 中未包含或高于 GB/T 39786 的密码应用要求,提出合规性特殊需求。

b) 重要信息资产保护特殊需求

针对信息系统中重要信息资产面临的实际安全风险,判断实施密码应用特殊措施的必要性,提出重要信息资产保护特殊需求。

活动输出:密码应用方案的密码应用特殊需求部分。

5.2.5 需求分析结果文档化

活动目标:

总结密码应用基本需求和密码应用特殊需求,形成密码应用方案的密码应用需求分析部分。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案的安全风险分析部分、密码应用基本需求部分、密码应用特殊需求部分。

活动描述:

根据安全风险分析、密码应用基本需求和密码应用特殊需求,确定信息系统的密码应用需求,形成密码应用需求分析。密码应用需求分析包含以下内容:

a) 安全风险分析;

b) 密码应用基本需求描述;

c) 密码应用特殊需求描述。

活动输出:密码应用方案的密码应用需求分析部分。

5.3 密码应用方案设计

5.3.1 总体策略设计

活动目标:

确定信息系统密码应用的总体设计目标和设计原则,以便开展信息系统密码应用的具体设计。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:信息系统责任单位总体安全策略文档,信息系统的立项、建设和管理文档,密码应用方案的系统概述部分、密码应用需求分析部分。

活动描述:

根据信息系统责任单位总体安全策略,结合信息系统建设规划及密码应用需求的实际情况,明确信息系统密码应用的设计目标和设计原则。

活动输出:密码应用方案的设计目标及原则部分。

5.3.2 密码应用技术方案设计

活动目标:

根据密码应用需求分析,提出信息系统需要实现的密码应用技术措施,用以指导信息系统密码应

用的具体建设。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案的密码应用需求分析部分。

活动描述:

根据密码应用需求分析,设计密码应用技术框架,分析物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全层面的密码保护对象,设计提出采用的密码应用技术措施。其中,在网络和通信安全层面,需要重点设计跨越不安全网络的通信信道的密码应用技术措施;在应用和数据安全层面,需要重点针对不同的信息系统,按其特定的安全需求,为其关键业务环节、重要业务数据、业务对象等设计密码安全机制,为用户选择登录认证机制,并且为这些机制的实现选择需遵循的密码国家及行业标准。

设计信息系统密钥管理体系,着重提出应用和数据层面的密钥种类及各类密钥全生命周期的技术实现和保护方式,明确信息系统密钥管理技术措施。

确定信息系统内的密码技术资源的共享情况和市场密码产品与密码服务的供给能力情况,并列出密码产品与密码服务需求清单。

确定信息系统采用密码功能时的应用系统改造需求。

活动输出:密码应用方案的密码应用技术方案部分。

5.3.3 密码应用安全管理方案设计

活动目标:

根据密码应用需求分析,结合原有管理模式和管理策略,形成统一的密码应用配套安全管理制度体系。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案的密码应用需求分析部分、密码应用技术方案部分。

活动描述:

根据信息系统密码应用需求分析,结合密码应用技术方案,确定密码应用配套安全管理制度体系。

活动输出:密码应用方案的密码应用安全管理方案部分。

5.3.4 合规性自查

活动目标:

对照 GB/T 39786 相应等级要求以及所属行业及关键信息基础设施相关要求,进行自查,确保密码应用技术方案及密码应用安全管理方案符合要求。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:所属行业及关键信息基础设施相关要求,密码应用方案的密码应用技术方案部分、密码应用安全管理方案部分。

活动描述:

按照 GB/T 39786 相应等级要求以及所属行业及关键信息基础设施相关要求,逐一列出要求项,形成密码应用合规性自查表,对方案设计中满足每项要求的情况逐一进行自评价。

活动输出:密码应用方案的安全与合规性分析部分。

5.3.5 实施保障方案设计

活动目标:

根据信息系统的建设规划以及密码应用的技术与安全管理设计,制定实施保障方案。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:信息系统总体描述文档,信息系统的立项、建设和管理文档,信息系统责任单位总体安全策略文档,密码应用方案的密码应用需求分析部分、密码应用技术方案部分、密码应用安全管理方案部分。

活动描述:

根据信息系统密码应用的具体设计,结合信息系统建设规划,确定信息系统密码应用的实施内容(包括但不限于采购、软硬件开发或改造、系统集成、综合调试、试运行),制定实施计划(包括但不限于实施路线图、进度计划、重要节点),确定保障措施(包括但不限于组织保障、人员保障、经费保障、质量保障、监督检查),并给出经费概算。

对于运行阶段信息系统的密码应用整改,还需要充分考虑采取各种措施,确保整改过程中信息系统稳定运行,保证业务的连续性。

活动输出:密码应用方案的实施保障方案部分。

5.3.6 设计结果文档化

活动目标:

将密码应用设计工作的结果文档化,最后形成一套指导信息系统责任单位密码应用工作的密码应用方案。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案的系统概述部分、密码应用需求分析部分、设计目标及原则部分、密码应用技术方案部分、密码应用安全管理方案部分、安全与合规性分析部分、实施保障方案部分。

活动描述:

对密码应用设计工作的内容进行整理并形成信息系统密码应用方案。密码应用方案主要包含以下内容:

- a) 信息系统概述;
- b) 密码应用需求分析;
- c) 设计目标及原则;
- d) 密码应用技术方案;
- e) 密码应用安全管理方案;
- f) 安全与合规性分析;
- g) 实施保障方案。

活动输出:密码应用方案。

5.4 方案密评

活动目标:

对制定的密码应用方案组织开展密评,确保方案符合信息系统密码应用要求、符合需求。

参与角色:信息系统责任单位、密评机构、密码应用集成服务单位、密码管理部门。

活动输入:密码应用方案。

活动描述:

本活动主要包括以下子活动内容。

- a) 方案评估

信息系统责任单位在初步确定密码应用方案后,对密码应用方案组织开展评估,形成方案密评报告。

委托商用密码应用安全性评估机构对方案进行评估时,密评机构以包括但不限于访谈、文档审查或必要情形下现场调查的方式确认方案的合规性和可实施性。密评机构在评估过程中关注密码应用方案是否充分涵盖信息系统中需要进行商用密码应用建设或改造的对象、是否充分分析信息系统中可能存在的密码应用安全风险,关注密码应用方案中采用的密码算法、密码技术、密钥管理、密码产品和密码服务是否符合 GB/T 39786 的要求。

b) 方案复评

未通过密评的密码应用方案,根据评估结果进行修改后,再次开展方案评估,形成方案密评报告。

c) 方案及评估结果备案

密码应用方案完成评估后,信息系统责任单位将密码应用方案和方案密评结果报送密码管理部门进行备案。

活动输出:方案密评报告。

6 信息系统密码应用建设

6.1 建设阶段的工作流程

信息系统密码应用建设阶段的目标是按照信息系统密码应用方案,制定密码建设方案,落实密码应用。信息系统密码应用建设阶段的工作流程见图 3。

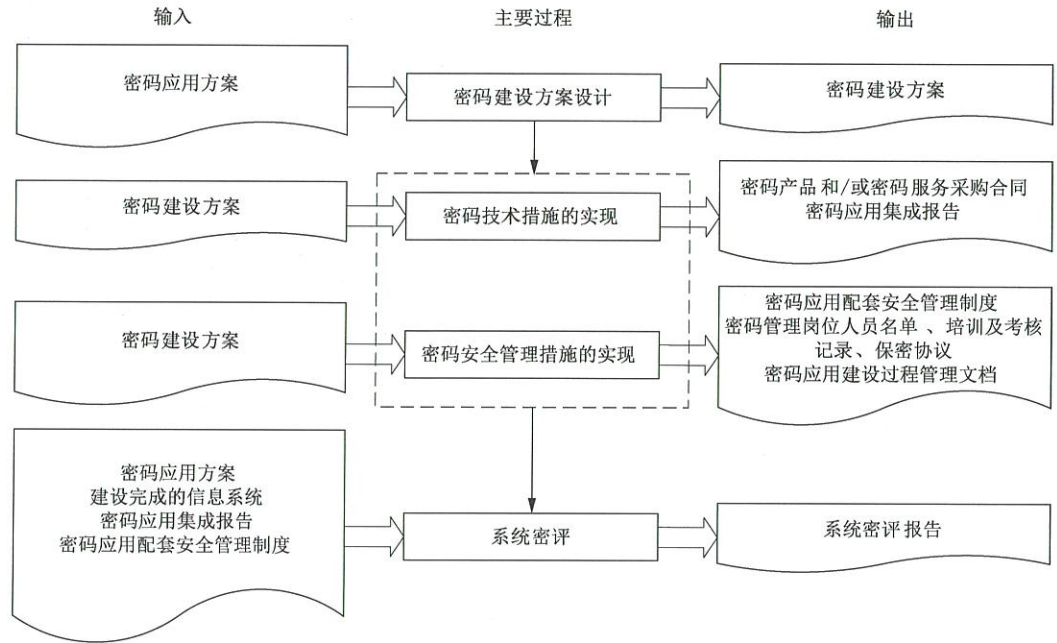


图 3 信息系统密码应用建设阶段的工作流程

6.2 密码建设方案设计

6.2.1 密码应用技术措施实现内容的设计

活动目标:

对密码应用方案中确定的密码产品或密码服务提出具体要求,并根据要求选择所需的密码产品或密码服务。

参与角色:信息系统责任单位、密码应用集成服务单位、密码产品和服务提供单位。

活动输入:密码应用方案。

活动描述：

本活动主要包括以下子活动内容。

a) 应用系统设计改造分析

分析信息系统采用密码功能所引发的应用系统设计或改造需求,确定应用系统设计或改造涉及的功能模块,形成应用系统设计或改造联调测试对接方案。

b) 密码部署方案设计

根据密码应用方案、应用系统设计或改造联调测试对接方案,确定密码产品或密码服务的具体部署方案。

c) 密码产品与密码服务采购清单确定

按照密码产品与密码服务需求清单,调研分析密码产品与密码服务的市场、供应商资质、产品或服务类型,形成密码产品与密码服务采购清单。

活动输出:密码建设方案的密码应用技术措施实现内容部分。

6.2.2 密码应用安全管理措施实现内容的设计

活动目标：

根据信息系统责任单位安全管理需要,提出与密码应用安全管理措施相适应的管理实施内容,以保证在密码应用技术措施建设的同时,密码安全管理得以同步建设。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案。

活动描述：

本活动主要包括以下子活动内容：

结合信息系统密码应用安全管理需要和密码应用技术措施建设内容,确定密码应用安全管理建设的范围和内 容,同时注意与信息系统原有安全管理制的协调性。密码应用安全管理设计的内容主要考虑:管理制度、人员管理、建设运行和应急处置。

活动输出:密码建设方案的密码应用安全管理措施实现内容部分。

6.2.3 设计结果文档化

活动目标：

汇总密码应用技术措施实现内容、密码应用安全管理措施实现内容,同时考虑工时和成本,最后形成密码建设方案。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案,密码建设方案的密码应用技术措施实现内容部分、密码应用安全管理措施实现内容部分。

活动描述：

综合分析密码应用技术措施实现内容、密码应用安全管理措施实现内容,形成密码建设方案。

活动输出:密码建设方案。

6.3 密码应用技术措施的实现

6.3.1 密码产品与密码服务采购

活动目标：

按照密码建设方案中对密码产品与密码服务的具体要求进行采购。

参与角色:信息系统责任单位、密码应用集成服务单位、密码产品和服务提供单位。

活动输入:密码建设方案。

活动描述:

按照国家法律法规和行业要求,确定密码产品与密码服务采购清单中各项密码产品与密码服务的提供单位,签订采购合同。

活动输出:密码产品和/或密码服务采购合同。

6.3.2 密码应用集成

活动目标:

将不同的密码产品和密码服务进行集成,依据密码建设方案,将密码产品、密码服务与各种应用系统综合、整合成为一个系统。

参与角色:信息系统责任单位、密码应用集成服务单位,密码产品和服务提供单位。

活动输入:密码建设方案。

活动描述:

本活动主要包括以下子活动内容。

a) 改造集成

依据密码建设方案,完成应用系统改造,将密码产品和密码服务与各种改造后的应用系统综合、整合成为一个系统,确保系统无缝对接。

对于运行阶段信息系统的密码应用整改,需要确保密码应用集成活动中信息系统稳定运行,保证业务的连续性。如有密码产品或密码服务需要退出使用或替换,需重点关注其密钥备份、恢复、销毁操作的安全。

b) 集成测试

对集成的信息系统密码应用进行测试,必要时委托第三方开展。

c) 试运行

信息系统责任单位确认测试通过后,对信息系统密码应用开展试运行,及时发现并处理问题。试运行结束后,形成信息系统密码应用集成报告。

活动输出:密码应用集成报告。

6.4 密码应用安全管理措施的实现

6.4.1 密码应用配套安全管理制度的制定

活动目标:

根据信息系统密码应用建设的实际情况,制定密码应用配套安全管理制度。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码建设方案。

活动描述:

根据信息系统建设的实际情况和密码应用安全管理措施,制定密码应用配套安全管理制度,主要包括:人员管理制度、密钥管理制度、密码应用建设运维制度、密码应用应急管理制度、密码产品及密码介质管理制度。根据密码应用实际情况,按需建立密码应用操作规程,设计操作记录表单,对密码管理人员的日常工作提供操作指导。

活动输出:密码应用配套安全管理制度。

6.4.2 密码管理岗位和人员的设置

活动目标:

根据信息系统的实际情况,通过岗位设置和岗位培训以及各种资源的配备,确保密码管理人员具有与密码管理岗位职责相适应的技术能力和管理能力,为信息系统的密码管理提供组织上的保障。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用配套安全管理制度。

活动描述:

本活动主要包括以下子活动内容。

a) 确定岗位和人员

根据密码应用配套安全管理制度设置密码管理岗位,确定密码管理岗位的具体人员。

b) 培训与考核

对密码管理人员进行专门培训和考核,确保其具有与其岗位职责相适应的技术能力和管理能力。

c) 签订保密协议

与关键人员签订保密协议。

活动输出:密码管理岗位人员名单、培训及考核记录、保密协议。

6.4.3 建设过程管理

活动目标:

在信息系统密码应用的规划和建设中,对密码应用工程的质量、进度、文档和变更工作进行监督控制和科学管理。

参与角色:信息系统责任单位、密码应用集成服务单位、密码产品和服务提供单位。

活动输入:密码建设方案。

活动描述:

本活动主要包括以下子活动内容。

a) 信息系统密码应用建设进度管理

监督信息系统密码应用建设进度,对未按计划完成的项目活动提出预警,按期生成建设进度报告。

b) 信息系统密码应用建设质量管理

监督信息系统密码应用建设质量,对不符合质量要求的项目活动提出预警和整改要求,按期生成建设质量报告。

c) 信息系统密码应用建设文档管理

对信息系统密码应用建设过程中形成的项目文档进行管理。

活动输出:密码应用建设过程管理文档。

6.5 系统密评

活动目标:

信息系统投入运行前,信息系统责任单位对已经完成密码应用建设的信息系统开展密评,确保信息系统的密码应用措施符合相应要求。

参与角色:信息系统责任单位、密评机构、密码应用集成服务单位、密码管理部门。

活动输入:密码应用方案,建设完成的信息系统,密码应用集成报告,密码应用配套安全管理制度。

活动描述:

本活动主要包括以下子活动内容。

a) 开展评估

信息系统责任单位对信息系统密码应用建设情况组织开展密评,形成系统密评报告。

建议系统密评与网络安全等级测评、关键信息基础设施安全检测评估工作统筹考虑,协调开展。

b) 系统整改和复评

未通过系统密评的,信息系统责任单位对信息系统进行整改,整改完成后组织进行复评,形成系统密评报告。

c) 评估结果备案

信息系统完成密评后,信息系统责任单位将系统密评结果报送密码管理部门备案。

活动输出:系统密评报告。

7 信息系统密码应用运行

7.1 运行阶段的工作流程

信息系统密码应用运行阶段的目标是按照密码应用方案,执行信息系统运行的制度、策略等,确保信息系统密码应用的正常运行。

信息系统密码应用运行阶段的工作流程见图 4。

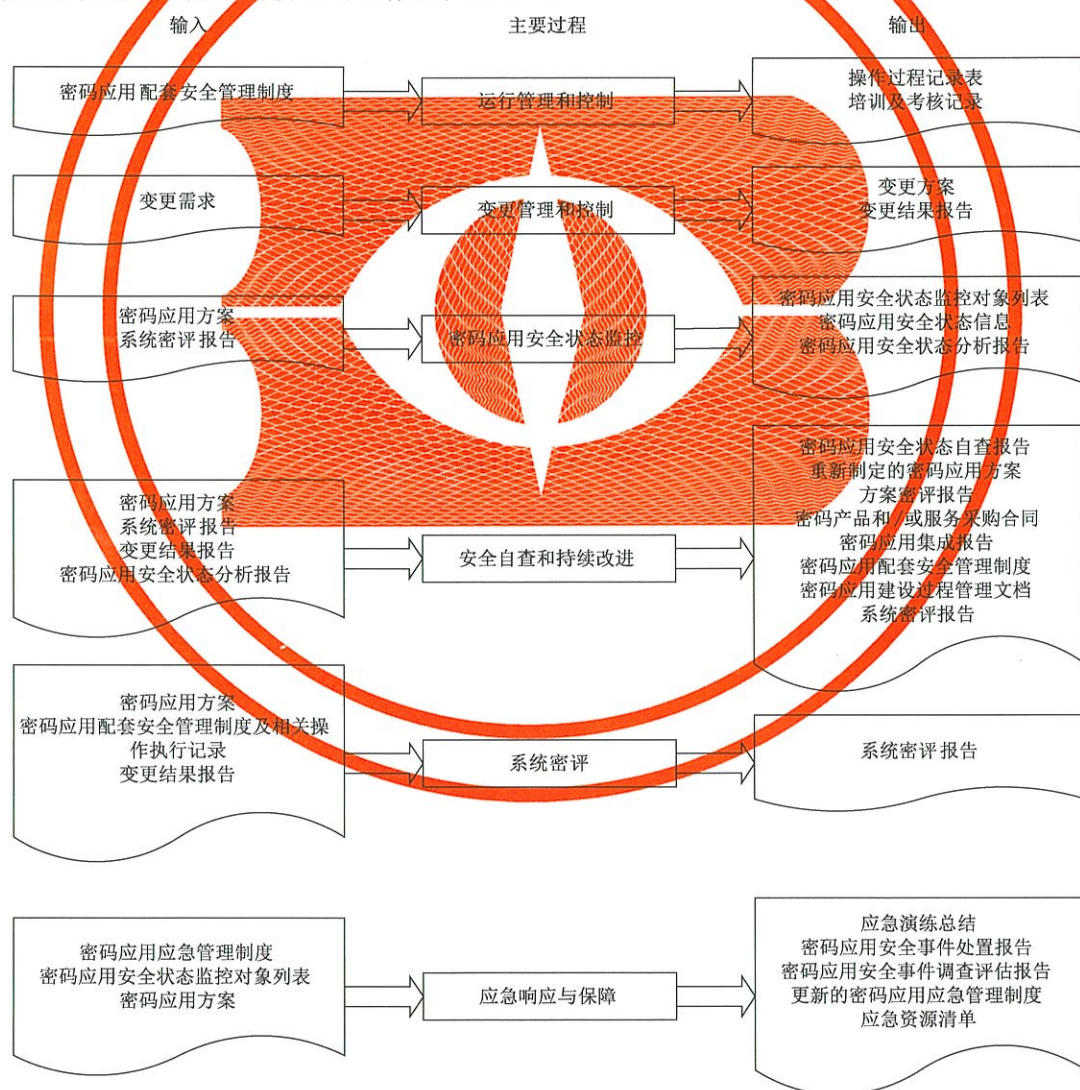


图 4 信息系统密码应用运行阶段的工作流程

7.2 运行管理和控制

7.2.1 运行管理过程控制

活动目标：

记录操作过程，确保对操作过程进行控制。

参与角色：信息系统责任单位、密码应用集成服务单位。

活动输入：密码应用配套安全管理制度。

活动描述：

本活动主要包括以下子活动内容。

a) 记录操作过程

记录运行操作人员的操作账户、操作内容、操作时间，并按国家行业要求存储操作记录。

b) 操作审计

定期对操作记录进行安全审计，及时发现违规操作或安全漏洞。

活动输出：操作过程记录表。

7.2.2 运行管理人员控制

活动目标：

定期对密码管理岗位人员进行培训、考核，确保其具备岗位所需专业技能。

参与角色：信息系统责任单位。

活动输入：密码应用配套安全管理制度。

活动描述：

根据密码应用配套安全管理制度，定期对密码管理人员进行专门培训和考核，确保其具备岗位所需专业技能。

活动输出：培训及考核记录。

7.3 变更管理和控制

7.3.1 变更需求和影响分析

活动目标：

通过对运行与维护过程中的变更需求和变更影响的分析，来确定变更的类别，计划后续的活动内容。

参与角色：信息系统责任单位、密码应用集成服务单位。

活动输入：变更需求。

活动描述：

本活动主要包括以下子活动内容。

a) 变更需求和影响分析

分析运行与维护过程中产生的变更需求（包括需求内容、需求来源、需求范围、需求迫切性，判断变更的必要性和可行性），并对变更可能存在的影响进行分析判断。

b) 变更方案制定

根据变更影响分析，制定变更方案。

活动输出：变更方案。

7.3.2 变更过程控制

活动目标：

确保运行与维护过程中的变更实施过程受到控制,各项变化内容进行记录,保证变更对业务的影响最小。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:变更方案。

活动描述：

本活动主要包括以下子活动内容。

a) 变更内容审核和审批

对变更目的、内容、影响、时间和地点以及人员权限进行审核,以确保变更合理、科学地实施。按照机构建立的审批流程对变更方案进行审批。

b) 变更试验与恢复预案

在有条件的情况下,按照变更方案,预先在试验验证系统中进行变更试验,验证变更方案的可行性。制定变更失败的应对预案,保证变更失败的情况下,可以恢复到变更前的状态。

c) 变更实施

按照变更方案,对信息系统密码应用实施变更操作,并对变更过程系统状态、各种操作活动的建立操作记录或日志。

变更活动中,如有密码产品或密码服务需要退出使用或替换,需要重点关注其密钥备份、恢复、销毁操作的安全。

d) 形成变更结果报告

收集变更过程各类文档,整理、分析和总结各类数据,形成变更结果报告,并归档保存。

活动输出:变更结果报告。

7.4 密码应用安全状态监控

7.4.1 监控对象确定

活动目标：

确定可能会对信息系统密码应用造成影响的因素,即确定密码应用安全状态监控的对象。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案,系统密评报告。

活动描述：

本活动主要包括以下子活动内容。

a) 安全关键点分析

对影响信息系统密码应用的关键要素进行分析,确定密码应用安全状态监控的对象(包括但不限于信息系统内所使用的密码产品、密钥、证书、密码算法、密码协议、密码服务及信息系统密码应用中使用的第三方组件,也可能包括法律法规、行业要求)。

b) 形成监控对象列表

根据确定的监控对象,分析监控的必要性和可行性、监控的开销和成本因素,形成监控对象列表。

活动输出:密码应用安全状态监控对象列表。

7.4.2 监控对象状态信息收集

活动目标：

收集密码应用安全状态监控的信息,识别和记录入侵、篡改行为,对信息系统的密码应用安全状态进行监控。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用安全状态监控对象列表。

活动描述:

采集监控对象的信息(包括但不限于操作和运行状态的实时信息,也可能包括来自外部环境的法律法规、行业要求的变更信息)。

活动输出:密码应用安全状态信息。

7.4.3 监控状态分析和报告

活动目标:

通过对密码应用安全状态信息进行分析,及时发现密码应用安全事件或安全变更需求,并对其影响程度和范围进行分析,形成密码应用安全状态结果分析报告。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用安全状态信息。

活动描述:

本活动主要包括以下子活动内容。

a) 状态分析

对采集到的监控信息进行分析,识别和记录异常和安全事件。

b) 影响分析

分析密码应用异常记录和安全事件,及其导致的安全状况变化,分析这些变化对安全的影响,并评估是否有必要作出响应。

c) 形成密码应用安全状态分析报告

对于需要作出响应的记录或事件,根据密码应用安全状态分析和影响分析的结果,形成密码应用安全状态分析报告,上报密码应用安全事件或提出变更需求。

活动输出:密码应用安全状态分析报告。

7.5 安全自查和持续改进

7.5.1 密码应用安全状态自查

活动目标:

对密码应用安全状态进行自查,及时检查、总结、调整现有的密码应用措施,确保信息系统的各项密码技术和管理措施满足相应密码应用安全要求。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案,系统密评报告,变更结果报告,密码应用安全状态分析报告。

活动描述:

本活动主要包括以下子活动内容。

a) 确定自查对象和自查方法

确定密码应用安全状态自查的范围,明确自查的对象、方法和自查工具。

b) 制定自查计划和自查方案

确定参与自查工作人员的角色和职责,制定自查计划和方案,准备密码应用安全状态自查需要的各类表单和工具。

c) 自查实施

按照密码应用安全状态自查计划进行自查,记录各种自查活动的结果数据,分析密码应用措施的有效性、密码应用安全事件产生的可能性和信息系统密码应用的实际改进需求。

d) 自查结果和报告

总结密码应用安全状态自查的结果,提出改进建议,生成密码应用安全状态自查报告,并将密码应用安全状态自查过程各类文档、资料归档保存。

活动输出:密码应用安全状态自查报告。

7.5.2 密码应用整改

活动目标:

针对自查结果中存在的安全风险进行整改,保证信息系统密码应用的合规性、正确性、有效性。

参与角色:信息系统责任单位、密码应用集成服务单位、密评机构。

活动输入:密码应用安全状态自查报告。

活动描述:

本活动主要包括以下子活动内容。

a) 确定整改策略

根据密码应用安全状态自查结果,确定密码应用整改的策略。

如果信息系统发生重大调整,需要修改密码应用方案时,则重新进入规划阶段,重新开始信息系统密码应用实施过程;如果信息系统因需求变化、未通过密评导致局部调整,不需要修改密码应用方案的,则重新进入建设阶段,进行密码应用整改。

b) 方案整改

对于需要修改密码应用方案的信息系统,重新进入规划阶段,根据标准、密码应用需求以及前期密评的整改建议,重新制定密码应用方案并组织开展方案密评。具体流程参见第5章。

c) 整改实施

对于不需要修改密码应用方案或重新制定的密码应用方案通过密评的信息系统,根据密码应用方案制定密码建设方案并开展建设,组织开展系统密评。具体流程参见第6章。

活动输出:重新制定的密码应用方案,方案密评报告,密码产品和/或密码服务采购合同,密码应用集成报告,密码应用配套安全管理制度,密码应用建设过程管理文档,系统密评报告。

7.6 系统密评

活动目标:

信息系统责任单位对运行中的信息系统定期组织开展密评,确保信息系统的密码应用措施符合相应的安全要求。

参与角色:信息系统责任单位、密评机构。

活动输入:密码应用方案,密码应用配套安全管理制度及操作执行记录,变更结果报告。

活动描述:

本活动主要包括以下子活动内容。

a) 开展评估

信息系统责任单位定期对信息系统密码应用实施情况组织开展密评。

b) 系统整改

信息系统责任单位参考评估报告,分析确定整改需求,并对信息系统进行整改,整改期间需保证系统的安全性。

c) 评估报告备案

信息系统完成密评后,信息系统责任单位将评估结果报送密码管理部门备案。

活动输出:系统密评报告。

7.7 应急响应与保障

7.7.1 应急准备

活动目标:

根据密码应用应急策略,开展培训宣贯和应急演练。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用应急管理制度。

活动描述:

本活动主要包括以下子活动内容。

a) 培训宣贯

针对应急策略涉及的密码操作和管理人员,制定专项培训计划,培训宣贯内容包括应急职责、合作和分工、应急策略启动条件及流程。

b) 应急演练

明确应急策略演练的规模、方式、范围、内容、组织、评估、总结,并按照策略开展演练。

活动输出:应急演练总结。

7.7.2 应急监测与响应

活动目标:

监控和收集与密码应用相关的异常安全状态信息,识别和记录与密码应用相关的入侵行为,对密码应用的安全状态进行监控,并根据应急策略的启动条件研判是否启动应急程序,开展应急响应处置工作。

参与角色:信息系统责任单位、密码应用集成服务单位,密码产品和服务提供单位。

活动输入:密码应用安全状态监控对象列表,密码应用应急管理制度。

活动描述:

本活动主要包括以下子活动内容。

a) 异常状态信息收集

异常状态信息收集见 7.4.2。

b) 异常状态分析

对采集到的监控信息进行分析,识别密码应用安全事件,分析其导致的安全状况变化以及这些变化对安全的影响,并根据应急策略评估是否有必要作出应急响应。

c) 应急处置和上报

对于应启动应急策略的密码应用安全事件,按照相应的应急策略进行处置。对未知安全事件的处置,可根据安全事件的实际情况制定应急策略(包括安全事件处置方法以及应采取的措施),并按照应急策略对安全事件进行处置。同时,及时向信息系统主管部门及归属的密码管理部门报告。

d) 安全事件总结和报告

一旦密码应用安全事件得到解决,对于未知的安全事件进行事件记录,分析记录信息并补充所需信息,使安全事件成为已知事件,并文档化;对安全事件处置过程进行总结,制定安全事件处置报告,并向有关部门报告。

活动输出:密码应用安全事件处置报告。

7.7.3 后期评估与改进

活动目标:

对密码应用安全事件的原因、处置过程进行调查分析,并根据分析结果进行责任认定及制定改进和/或预防措施。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用方案,密码应用应急管理制度,密码应用安全事件处置报告。

活动描述:

本活动主要包括以下子活动内容。

a) 调查评估

对于应急响应过程进行调查,评估应急过程的合规性、处置及时性。调查密码应用安全事件原因,追溯安全责任,并形成密码应用安全事件调查评估报告。

b) 改进预防

根据密码应用安全事件调查评估报告,分析并改进应急策略,结合实际情况进行落实,并组织开展应急策略培训。

活动输出:密码应用安全事件调查评估报告,更新的密码应用应急管理制度。

7.7.4 应急保障

活动目标:

根据应急资源需求,做好应急资源准备。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用应急管理制度。

活动描述:

根据应急资源需求,做好应急资源准备,确保应急资源充足。

活动输出:应急资源清单。

8 信息系统密码应用终止

8.1 终止阶段工作流程

信息系统密码应用终止阶段的目标是确保信息系统密码应用的安全终止。当信息系统密码应用被转移、终止或废弃时需正确处理信息系统密码应用中的重要数据,以确保信息系统的安全。在信息系统密码应用生命周期中,有些信息系统密码应用并不是真正意义上的废弃,而是改进技术或转变业务到新的信息系统密码应用中。对于这些信息系统密码应用,在终止处理过程中需确保信息转移、设备迁移和介质销毁方面的安全。信息系统密码应用终止阶段的工作流程见图 5。

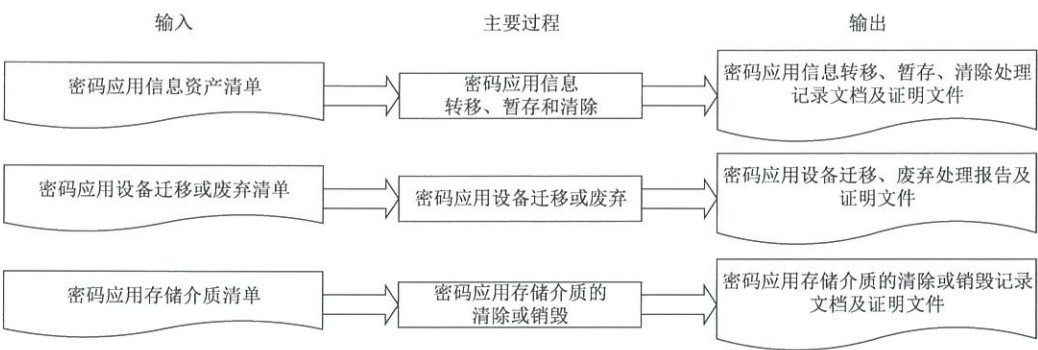


图 5 信息系统密码应用终止阶段流程图

8.2 密码应用信息转移、暂存和清除

活动目标：

在信息系统密码应用终止处理过程中,对于可能会在另外的信息系统密码应用中使用的信息采取适当的方法将其安全地转移或暂存到可以恢复的介质中,确保将来可以继续使用,同时采用安全的方法清除要终止的信息系统密码应用中的信息。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用信息资产清单。

活动描述：

本活动主要包括以下子活动内容。

a) 识别要转移、暂存和清除的信息资产

根据要终止的信息系统密码应用的信息资产清单,识别重要信息资产、所处的位置以及当前状态,列出需转移、暂存和清除的信息资产的清单。

b) 信息资产转移、暂存和清除

根据密码应用信息资产的重要程度制定密码应用信息资产的转移、暂存清除的方法和过程。如果是涉密信息,则按照国家相关部门的规定进行转移、暂存和清除。

c) 处理过程记录

记录密码应用信息转移、暂存和清除的过程(包括参与的人员,转移、暂存和清除的方式以及目前信息所处的位置)。

活动输出:密码应用信息转移、暂存、清除处理记录文档及证明文件。

8.3 密码应用设备迁移或废弃

活动目标：

确保信息系统密码应用终止后迁移或废弃的设备内不包括重要数据,对设备的处理方式需符合国家相关部门的要求。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用设备迁移或废弃清单。

活动描述：

本活动主要包括以下子活动内容。

a) 设备识别

根据要终止的信息系统密码应用的设备清单,识别要被迁移或废弃的硬件设备、所处的位置以及当前状态,列出需迁移、废弃的设备的清单。

b) 制定设备处理方案

根据规定和实际情况制定设备处理方案(包括设备迁移方法、设备废弃方法和重要数据清除方法)。

c) 处理方案审批

设备处理方案依据组织的的安全管理制度经过主管领导审查和批准。

d) 设备处理和记录

根据设备处理方案对设备进行处理,如果是涉密信息的设备,其处理过程需符合国家相关部门的规定;记录设备处理过程(包括参与的人员、处理的方式、是否有残余信息的检查结果)。

活动输出:密码应用设备迁移、废弃处理报告及证明文件。

8.4 密码应用存储介质的清除或销毁

活动目标:

通过采用合理的方式对信息系统密码应用中的计算机介质(包括磁带、磁盘、打印结果和文档)进行信息清除或销毁处理,防止介质内的重要数据泄露。

参与角色:信息系统责任单位、密码应用集成服务单位。

活动输入:密码应用存储介质清单。

活动描述:

本活动主要包括以下活动内容。

a) 识别要清除或销毁的介质

根据要终止的信息系统密码应用的存储介质清单,识别载有重要数据的密码应用存储介质、所处的位置以及当前状态,列出需清除或销毁的密码应用存储介质清单。

b) 确定存储介质处理方法和流程

根据密码应用存储介质所承载信息的重要程度确定对密码应用存储介质的处理方式和处理流程(包括数据清除和存储介质销毁)。对于存储涉密信息的介质需按照国家相关部门的规定进行处理。

c) 处理方案审批

密码应用存储介质的处理方式和处理流程的处理方案需经过主管领导审查和批准。

d) 存储介质处理和记录

根据密码应用存储介质处理方案对存储介质进行处理,记录处理过程(包括参与的人员、处理的方式、是否有残余信息的检查结果)。

活动输出:密码应用存储介质的清除或销毁记录文档及证明文件。

附录 A

(规范性)

主要过程及其活动和输入输出

信息系统密码应用实施的主要过程及其活动和输入输出见表 A.1。

表 A.1 信息系统密码应用实施的主要过程及其活动和输入输出

主要阶段	主要过程	活动	活动输入	活动输出
信息系统密码应用规划	密码应用需求分析	信息系统现状分析	单位情况说明文档 信息系统的立项、建设和管理文档 信息系统总体描述文档	密码应用方案的信息系统概述部分
		安全风险分析	信息系统总体描述文档 信息系统资产、威胁、脆弱性分析文档	密码应用方案的安全风险分析部分
		密码应用基本需求的确定	密码应用方案的安全风险分析部分	密码应用方案的密码应用基本需求部分
		密码应用特殊需求的确定	密码应用方案的安全风险分析部分 所属行业及关键信息基础设施相关要求文档	密码应用方案的密码应用特殊需求部分
		需求分析文档化	密码应用方案的安全风险分析、密码应用基本需求、密码应用特殊需求部分	密码应用方案的密码应用需求分析部分
	密码应用方案设计	总体策略设计	单位总体安全策略文档 信息系统的立项、建设和管理文档 密码应用方案的系统概述部分、密码应用需求分析部分	密码应用方案的设计目标及原则部分
		密码应用技术方案设计	密码应用方案的密码应用需求分析部分	密码应用方案的密码应用技术方案部分
		密码应用安全管理方案设计	密码应用方案的密码应用需求分析部分、密码应用技术方案部分	密码应用方案的密码应用安全管理方案部分
		合规性自查	所属行业及关键信息基础设施相关要求文档 密码应用方案的密码应用技术方案部分、密码应用安全管理方案部分	密码应用方案的安全与合规性分析部分
		实施保障方案设计	信息系统总体描述文档 信息系统的立项、建设和管理文档 单位总体安全策略文档 密码应用方案的密码应用需求分析部分、密码应用技术方案部分、密码应用安全管理方案部分 密码应用配套安全管理制度	密码应用方案的实施保障方案部分

表 A.1 信息系统密码应用实施的主要过程及其活动和输入输出 (续)

主要阶段	主要过程	活动	活动输入	活动输出
信息系统密码应用规划	密码应用方案设计	设计结果文档化	密码应用方案的系统概述部分、密码应用需求分析部分、设计目标及原则部分、密码应用技术方案部分、密码应用安全管理方案部分、安全与合规性分析部分、实施保障方案部分	密码应用方案
	方案密评		密码应用方案	方案密评报告
信息系统密码应用建设	密码建设方案设计	密码应用技术措施实现内容的设计	密码应用方案	密码建设方案的密码应用技术措施实现内容部分
		密码应用安全管理措施实现内容的设计	密码应用方案 密码应用配套安全管理制度	密码建设方案的密码应用安全管理措施实现内容部分
		设计结果文档化	密码应用方案 密码建设方案的密码应用技术措施实现内容、密码应用安全管理措施实现内容部分	密码建设方案
	密码应用技术措施的实现	密码产品与服务采购	密码建设方案	密码产品和服务采购合同
		密码应用集成	密码建设方案	密码应用集成报告
信息系统密码应用建设	密码应用安全管理措施的实现	密码应用配套安全管理制度的制定	密码建设方案	密码应用配套安全管理制度
		密码管理岗位和人员的设置	密码应用配套安全管理制度	密码管理岗位人员名单、培训及考核记录、保密协议
		建设过程管理	密码建设方案	密码应用建设过程管理文档
	系统密评		密码应用方案 建设完成的信息系统 密码应用集成报告 密码应用配套安全管理制度	系统密评报告
信息系统密码应用运行	运行管理和控制	运行管理过程控制	密码应用配套安全管理制度	操作过程记录表
		运行管理人员控制	密码应用配套安全管理制度	培训及考核记录
	变更管理和控制	变更需求和影响分析	变更需求	变更方案
		变更过程控制	变更方案	变更结果报告

表 A.1 信息系统密码应用实施的主要过程及其活动和输入输出 (续)

主要阶段	主要过程	活动	活动输入	活动输出
信息系统密码应用运行	密码应用安全状态监控	监控对象确定	密码应用方案 系统密评报告	密码应用安全状态监控对象列表
		监控对象状态信息收集	密码应用安全状态监控对象列表	密码应用安全状态信息
		监控状态分析和报告	密码应用安全状态信息	密码应用安全状态分析报告
	安全自查和持续改进	密码应用安全状态自查	密码应用方案 系统密评报告 变更结果报告 密码应用安全状态分析报告	密码应用安全状态自查报告
	安全自查和持续改进	密码应用整改	密码应用安全状态自查报告	重新制定的密码应用方案 方案密评报告 密码产品和/或密码服务采购合同 密码应用集成报告 密码应用配套安全管理制度 密码应用建设过程管理文档 系统密评报告
	系统密评		密码应用方案 密码应用配套安全管理制度及操作执行记录 变更结果报告	系统密评报告
	应急响应与保障	应急准备	密码应用应急管理制度	应急演练总结
		应急监测与响应	密码应用安全状态监控对象列表 密码应用应急管理制度	密码应用安全事件处置报告
		后期评估与改进	密码应用方案 密码应用应急管理制度 密码应用安全事件处置报告	密码应用安全事件调查评估报告 更新的密码应用应急管理制度
		应急保障	密码应用应急管理制度	应急资源清单
信息系统密码应用终止	密码应用信息数据转移、暂存和清除	密码应用信息资产清单	密码应用信息资产清单	密码应用信息转移、暂存、清除处理记录文档及证明文件
	密码应用设备迁移或废弃	密码应用设备迁移或废弃清单	密码应用设备迁移或废弃清单	密码应用设备迁移、废弃处理报告及证明文件
	密码应用存储介质的清除或销毁	密码应用存储介质清单	密码应用存储介质清单	密码应用存储介质的清除或销毁记录文档及证明文件

注：表格中黑体字部分表示最终输出成果文档。

参 考 文 献

- [1] GB/T 25058 信息安全技术 网络安全等级保护实施指南
 - [2] GB/T 28449 信息安全技术 网络安全等级保护测评过程指南
-