ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43206—2023

信息安全技术
信息系统密码应用测评要求

Information security technology—Testing and evaluation requirements for information system cryptography application

2023-09-07 发布　　2024-04-01 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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：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、公安部第三研究所、国家信息技术安全研究中心、中国电子科技集团公司第十五研究所、中国电子技术标准化研究院、国家信息中心、工业和信息化部电子第五研究所、中国科学院软件研究所、北京市政务信息安全保障中心(北京信息安全测评中心)、北京国家数字金融技术检测中心有限公司、深圳市网安计算机安全检测技术有限公司、道普信息技术有限公司、国电南京自动化股份有限公司、浙江东安检测技术有限公司、北京银联金卡科技有限公司、智巡密码(上海)检测技术有限公司、哈尔滨工业大学(深圳)、安徽科测信息技术有限公司、新疆量子通信技术有限公司。

本文件主要起草人：罗鹏、肖秋林、马原、张立花、许长伟、陈天宇、黄晶晶、郑昉昱、田敏求、王兵、刘健、杨宏志、吴冬宇、陆臻、张宇翔、李升、任金强、黎水林、李大为、李宏卓、张五一、张晓溪、杨辰、蔡一鸣、孙鑫、高锐、吕娜、宋玲娓、郭守坤、何双羽、杨龙、李霞、王国朝、胡盖、胡燕雄、沈汀、张绍博、韩玮。

信息安全技术
信息系统密码应用测评要求

1 范围

本文件规定了信息系统第一级到第四级密码应用的通用测评要求、技术测评要求、管理测评要求，并给出了整体测评要求、风险分析和评价、测评结论的要求。

注：本文件描述的信息系统密码应用等级与 GB/T 39786—2021 规定的密码应用等级一致，其中第五级密码应用的测评要求不在本文件中描述。

本文件适用于指导、规范信息系统密码应用安全性评估工作中的测评活动。

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 25069—2022 信息安全技术 术语

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069—2022、GB/T 39786—2021 和 GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

密码应用安全性评估人员 commercial cryptography application security evaluation staff

通过国家密码管理部门认可的考核或具有密码技术应用员、密码工程技术人员职业技能等级证书，从事密码应用安全性评估的人员。

注：简称“密评人员”。

3.2

核查 examine

密评人员对测评对象进行访谈、文档审查、实地查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

注：核查时可选用的测评方式以及方式的选用说明参考 GM/T 0116—2021。

[来源：GB/T 25069—2022，3.237，有修改]

3.3

测评单元 unit of testing and evaluation

一组相对独立和完整的测评内容，由测评指标、测评对象、测评实施和结果判定组成。

3.4

测评指标　index of testing and evaluation

测评单元中第一级到第四级密码应用测评的具体要求。

3.5

测评对象　target of testing and evaluation

测评单元中密码应用的测评实施对象。

注：主要包括物理安防设施、通信信道、密码产品、通用设备、应用、重要数据、人员、制度文档等。测评对象基于密码应用方案和信息系统保护目标的实际安全需求确定，具体确定方法参考 GM/T 0116—2021。

4　通则

本文件对信息系统各密码应用等级的测评指标以“应”“宜”“可”方式进行描述，密评人员在开展实际测评时，按照如下方法确定是否纳入测评和结果判定范围。

a）　对于“应”的条款，密评人员应按照第 6 章和第 7 章中相应的测评指标要求进行测评和结果判定。

如根据信息系统的密码应用方案和方案评估意见，密评人员应判定信息系统确实不存在与测评指标相关的密码应用需求，则相应测评指标为“不适用”；否则，相关条款纳入测评和结果判定范围。

b）　对于“宜”的条款，密评人员应确认信息系统是否具有已通过评估的密码应用方案。

1）　如信息系统没有通过评估的密码应用方案，或方案评估意见中未对“不适用”项作出明确说明，则“宜”的条款纳入测评和结果判定范围。

2）　如信息系统有已通过评估的密码应用方案，且方案评估意见中对“宜”条款作出了明确说明，则密评人员应根据信息系统的密码应用方案和方案评估意见决定是否纳入测评和结果判定范围。

——如纳入测评和结果判定范围，则密评人员应按照第 6 章和第 7 章相应的测评指标要求进行测评和结果判定。

——如未纳入测评和结果判定范围，且判定信息系统确实不存在与测评指标相关的密码应用需求时，则相应测评指标为“不适用”。

——如未纳入测评和结果判定范围，但信息系统有与测评指标相关的密码应用需求，密评人员应根据信息系统的密码应用方案和方案评估意见，在测评中进一步核实该信息系统是否满足密码应用方案描述的风险控制措施使用条件，且信息系统的实施情况与所描述的风险控制措施是否一致，并在密码应用安全性评估报告中体现核实过程和结果。如满足使用条件且风险控制措施一致，该测评指标为“不适用”；如不满足使用条件或风险控制措施不一致，密评人员应按照第 6 章和第 7 章中相应的测评指标要求进行测评和结果判定。

c）　对于“可”的条款，由信息系统责任方自行决定是否纳入测评和结果判定范围。

1）　如信息系统责任方确认纳入测评和结果判定范围，且密评人员经核实后判定信息系统不存在与测评指标相关的密码应用需求，则密评人员应在密码应用安全性评估报告中体现核实过程和结果，相应测评指标为“不适用”。

2）　如信息系统责任方确认纳入测评和结果判定范围，且密评人员经核实后判定信息系统存在与测评指标相关的密码应用需求，则密评人员应按照第 6 章和第 7 章中相应的测评指标要求进行测评和结果判定。

如信息系统通过评估的密码应用方案要求高于其自身对应等级的测评指标要求，则密评人员应按照密码应用方案要求进行测评。例如，密码应用方案要求第三级的信息系统部分指标按照第四级进行规划、建设、运行，则对应指标按照密码应用等级第四级进行测评，并在密码应用安全性评估报告中记录。

5 通用测评要求

5.1 密码算法

5.1.1 测评指标

信息系统中使用的密码算法符合法律、法规的规定和密码相关国家标准、行业标准的有关要求（适用于第一级到第四级）。

5.1.2 测评对象

信息系统中使用的密码算法。

5.1.3 测评实施

了解信息系统中使用的密码算法的名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查信息系统中使用的密码算法是否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

5.2.1 测评指标

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（适用于第一级到第四级）。

5.2.2 测评对象

信息系统中使用的密码技术。

5.2.3 测评实施

了解信息系统中使用的密码技术的名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查信息系统中使用的密码技术是否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。

5.3 密码产品

5.3.1 测评指标

本单元测评指标如下。

信息系统中使用的密码产品符合法律法规和密码相关国家标准、行业标准的相关要求（适用于第一级到第四级）。

信息系统中使用的密码产品如遵循密码模块相关标准，则应：

——达到密码模块安全等级一级及以上安全要求（适用于第二级）；

——达到密码模块安全等级二级及以上安全要求（适用于第三级）；

——达到密码模块安全等级三级及以上安全要求（适用于第四级）。

5.3.2 测评对象

信息系统中使用的密码产品。

5.3.3 测评实施

了解信息系统中使用的密码产品的型号和版本等配置信息，核查密码产品是否经商用密码认证机构认证合格，并核查密码产品的使用是否满足其安全运行的条件，例如其安全策略或使用手册说明的部署条件。遵循了密码模块相关标准的密码产品，还要核查其是否满足密码模块相应安全等级及以上安全要求。

5.4 密码服务

5.4.1 测评指标

信息系统中使用的密码服务符合法律法规的相关要求(适用于第一级到第四级)。

5.4.2 测评对象

信息系统中使用的密码服务。

5.4.3 测评实施

核查信息系统中使用的密码服务是否符合法律法规的相关要求。

5.5 密钥管理

5.5.1 测评指标

本单元测评指标如下：

——信息系统密钥管理使用的密码产品、密码服务符合法律法规和密码相关国家标准、行业标准的要求(适用于第一级到第四级)；

——信息系统密钥管理应符合密码相关国家标准和行业标准的要求(适用于第一级到第四级)。

5.5.2 测评对象

信息系统密钥管理使用的密码产品、密码服务以及密钥管理实现。

5.5.3 测评实施

本单元测评实施如下：

a) 核查密钥管理使用的密码产品、密码服务是否满足 5.3 和 5.4 的要求；

b) 核查信息系统密钥管理实现是否安全、正确、有效。例如：非公开密钥是否能被非授权访问、使用、泄露、修改和替换，公开密钥是否能被非授权修改和替换。详细测评实施要点可见附录 A。

6 技术测评要求

6.1 物理和环境安全

6.1.1 身份鉴别

6.1.1.1 测评指标

本单元测评指标如下：

——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（适用于第一级）；

——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（适用于第二级到第三级）；

——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（适用于第四级）。

6.1.1.2 测评对象

信息系统所在机房等重要区域及其电子门禁系统。

6.1.1.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C）：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查电子门禁系统是否采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对重要区域进入人员进行身份鉴别，并验证进入人员身份真实性实现机制是否正确和有效。

6.1.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.1.1.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.1.1.3 c）测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.1.2 电子门禁记录数据存储完整性

6.1.2.1 测评指标

本单元测评指标如下：

——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（适用于第一级到第二级）；

——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（适用于第三级）；

——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（适用于第四级）。

6.1.2.2 测评对象

信息系统所在机房等重要区域及其电子门禁系统。

6.1.2.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C）：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对电子门禁系统进出记录数据进行存储完整性保护，并验证完整性保护机制是否正确和有效。

6.1.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.1.2.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.1.2.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.1.3 视频监控记录数据存储完整性

6.1.3.1 测评指标

本单元测评指标如下：

——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(适用于第三级)；

——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(适用于第四级)。

6.1.3.2 测评对象

信息系统所在机房等重要区域及其视频监控系统。

6.1.3.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对视频监控音像记录数据进行存储完整性保护，并验证完整性保护机制是否正确和有效。

6.1.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.1.3.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.1.3.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.2 网络和通信安全

6.2.1 身份鉴别

6.2.1.1 测评指标

本单元测评指标如下：

——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（适用于第一级）；

——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（适用于第二级）；

——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（适用于第三级）；

——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（适用于第四级）。

6.2.1.2 测评对象

信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品等。

6.2.1.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C）：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对通信实体进行身份鉴别（适用于第一级到第三级）/双向身份鉴别（适用于第四级），并验证通信实体身份真实性实现机制是否正确和有效。

6.2.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.2.1.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.2.1.3 c）测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.2.2 通信数据完整性

6.2.2.1 测评指标

本单元测评指标如下：

——可采用密码技术保证通信过程中数据的完整性（适用于第一级到第二级）；

——宜采用密码技术保证通信过程中数据的完整性（适用于第三级）；

——应采用密码技术保证通信过程中数据的完整性（适用于第四级）。

6.2.2.2 测评对象

信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品等。

6.2.2.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对通信过程中的数据进行完整性保护，并验证通信数据完整性保护机制是否正确和有效。

6.2.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.2.2.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.2.2.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.2.3 通信过程中重要数据的机密性

6.2.3.1 测评指标

本单元测评指标如下：

——可采用密码技术保证通信过程中重要数据的机密性(适用于第一级)；

——宜采用密码技术保证通信过程中重要数据的机密性(适用于第二级)；

——应采用密码技术保证通信过程中重要数据的机密性(适用于第三级到第四级)。

6.2.3.2 测评对象

信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品等。

6.2.3.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采用密码技术的加解密功能对通信过程中敏感信息或通信报文进行机密性保护，并验证敏感信息或通信报文机密性保护机制是否正确和有效。

6.2.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.2.3.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.2.3.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果

均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.2.4 网络边界访问控制信息的完整性

6.2.4.1 测评指标

本单元测评指标如下：

——可采用密码技术保证网络边界访问控制信息的完整性（适用于第一级到第二级）；

——宜采用密码技术保证网络边界访问控制信息的完整性（适用于第三级）；

——应采用密码技术保证网络边界访问控制信息的完整性（适用于第四级）。

6.2.4.2 测评对象

信息系统与网络边界外建立的网络通信信道，以及提供网络边界访问控制功能的设备或组件、密码产品等。

6.2.4.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C）：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对网络边界访问控制信息进行完整性保护，并验证网络边界访问控制信息完整性保护机制是否正确和有效。

6.2.4.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.2.4.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.2.4.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.2.5 安全接入认证

6.2.5.1 测评指标

本单元测评指标如下：

——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，确保接入设备身份的真实性（适用于第三级）；

——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（适用于第四级）。

6.2.5.2 测评对象

信息系统内部网络，以及提供设备入网接入认证功能的设备或组件、密码产品等。

6.2.5.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C):

a) 核查是否符合 5.1 和 5.2 的要求;

b) 核查是否符合 5.3、5.4 和 5.5 的要求;

c) 核查是否采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对从外部连接到内部网络的设备进行接入认证,并验证安全接入认证机制是否正确和有效。

6.2.5.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果 6.2.5.3 测评结果均为是,则该测评对象符合本单元的测评指标要求;如果 6.2.5.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

6.3 设备和计算安全

6.3.1 身份鉴别

6.3.1.1 测评指标

本单元测评指标如下:

——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(适用于第一级);

——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(适用于第二级);

——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(适用于第三级到第四级)。

6.3.1.2 测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备,以及提供身份鉴别功能的密码产品等。

6.3.1.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C):

a) 核查是否符合 5.1 和 5.2 的要求;

b) 核查是否符合 5.3、5.4 和 5.5 的要求;

c) 核查是否采用动态口令机制、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对设备操作人员等登录设备的用户进行身份鉴别,并验证登录设备的用户身份真实性实现机制是否正确和有效。

6.3.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.3.1.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.3.1.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.3.2 远程管理通道安全

6.3.2.1 测评指标

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(适用于第三级到第四级)。

6.3.2.2 测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备，以及提供安全的信息传输通道的密码产品等。

6.3.2.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查远程管理时是否采用密码技术建立安全的信息传输通道，包括身份鉴别、传输数据机密性和完整性保护，并验证远程管理信道所采用的密码技术实现机制是否正确和有效。

6.3.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.3.2.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.3.2.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.3.3 系统资源访问控制信息完整性

6.3.3.1 测评指标

本单元测评指标如下：

——可采用密码技术保证系统资源访问控制信息的完整性(适用于第一级到第二级)；

——宜采用密码技术保证系统资源访问控制信息的完整性(适用于第三级)；

——应采用密码技术保证系统资源访问控制信息的完整性(适用于第四级)。

6.3.3.2 测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备，以及提供完整性保护功能的密码产品等。

6.3.3.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对设备上系统资源访问控制信息进行完整性保护，并验证系统资源访问控制信息完整性保护机制是否正确和有效。

6.3.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.3.3.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.3.3.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.3.4 重要信息资源安全标记完整性

6.3.4.1 测评指标

本单元测评指标如下：

——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(适用于第三级)；

——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(适用于第四级)。

6.3.4.2 测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备，以及提供完整性保护功能的密码产品等。

6.3.4.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对设备中的重要信息资源安全标记进行完整性保护，并验证安全标记完整性保护机制是否正确和有效。

6.3.4.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.3.4.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.3.4.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.3.5 日志记录完整性

6.3.5.1 测评指标

本单元测评指标如下：

——可采用密码技术保证日志记录的完整性（适用于第一级到第二级）；

——宜采用密码技术保证日志记录的完整性（适用于第三级）；

——应采用密码技术保证日志记录的完整性（适用于第四级）。

6.3.5.2 测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备，以及提供完整性保护功能的密码产品等。

6.3.5.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C）：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对设备运行的日志记录进行完整性保护，并验证日志记录完整性保护机制是否正确和有效。

6.3.5.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.3.5.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.3.5.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.3.6 重要可执行程序完整性、重要可执行程序来源真实性

6.3.6.1 测评指标

本单元测评指标如下：

——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（适用于第三级）；

——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（适用于第四级）。

6.3.6.2 测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备，以及提供完整性保护和来源真实性功能的密码产品等。

6.3.6.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采用基于公钥密码算法的数字签名机制等密码技术对重要可执行程序进行完整性保护并实现其来源的真实性保护，并验证重要可执行程序完整性保护机制和其来源真实性实现机制是否正确和有效。

6.3.6.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.3.6.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.3.6.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.4 应用和数据安全

6.4.1 身份鉴别

6.4.1.1 测评指标

本单元测评指标如下：

——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(适用于第一级)；

——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(适用于第二级)；

——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(适用于第三级到第四级)。

6.4.1.2 测评对象

业务应用，以及提供身份鉴别功能的密码产品等。

6.4.1.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采用动态口令机制、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对应用登录用户进行身份鉴别，并验证应用系统用户身份真实性实现机制是否正确和有效。

6.4.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.4.1.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.4.1.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.4.2 访问控制信息完整性

6.4.2.1 测评指标

本单元测评指标如下：

——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(适用于第一级到第二级)；

——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(适用于第三级)；

——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(适用于第四级)。

6.4.2.2 测评对象

业务应用，以及提供完整性保护功能的密码产品等。

6.4.2.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采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对应用的访问控制信息进行完整性保护，并验证应用的访问控制信息完整性保护机制是否正确和有效。

6.4.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.4.2.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.4.2.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.4.3 重要信息资源安全标记完整性

6.4.3.1 测评指标

本单元测评指标如下：

——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(适用于第三级);
——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(适用于第四级)。

6.4.3.2 测评对象

业务应用,以及提供完整性保护功能的密码产品等。

6.4.3.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C):

a) 核查是否符合 5.1 和 5.2 的要求;
b) 核查是否符合 5.3、5.4 和 5.5 的要求;
c) 核查是否采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对应用的重要信息资源安全标记进行完整性保护,并验证安全标记完整性保护机制是否正确和有效。

6.4.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果 6.4.3.3 测评结果均为是,则该测评对象符合本单元的测评指标要求;如果 6.4.3.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

6.4.4 重要数据传输机密性

6.4.4.1 测评指标

本单元测评指标如下:

——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(适用于第一级);
——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(适用于第二级);
——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(适用于第三级到第四级)。

6.4.4.2 测评对象

业务应用,以及提供机密性保护功能的密码产品等。

6.4.4.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C):

a) 核查是否符合 5.1 和 5.2 的要求;
b) 核查是否符合 5.3、5.4 和 5.5 的要求;
c) 核查是否采用密码技术的加解密功能对重要数据在传输过程中进行机密性保护,并验证传输数据机密性保护机制是否正确和有效。

6.4.4.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.4.4.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.4.4.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.4.5 重要数据存储机密性

6.4.5.1 测评指标

本单元测评指标如下：

——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(适用于第一级)；

——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(适用于第二级)；

——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(适用于第三级到第四级)。

6.4.5.2 测评对象

业务应用，以及提供机密性保护功能的密码产品等。

6.4.5.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采用密码技术的加解密功能对重要数据在存储过程中进行机密性保护，并验证存储数据机密性保护机制是否正确和有效。

6.4.5.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.4.5.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.4.5.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.4.6 重要数据传输完整性

6.4.6.1 测评指标

本单元测评指标如下：

——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(适用于第一级);
——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(适用于第二级到第三级);
——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(适用于第四级)。

6.4.6.2 测评对象

业务应用,以及提供完整性保护功能的密码产品等。

6.4.6.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C):

a) 核查是否符合 5.1 和 5.2 的要求;
b) 核查是否符合 5.3、5.4 和 5.5 的要求;
c) 核查是否采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对重要数据在传输过程中进行完整性保护,并验证传输数据完整性保护机制是否正确和有效。

6.4.6.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果 6.4.6.3 测评结果均为是,则该测评对象符合本单元的测评指标要求;如果 6.4.6.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

6.4.7 重要数据存储完整性

6.4.7.1 测评指标

本单元测评指标如下:

——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(适用于第一级);
——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(适用于第二级到第三级);
——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(适用于第四级)。

6.4.7.2 测评对象

业务应用,以及提供完整性保护功能的密码产品等。

6.4.7.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C):

a) 核查是否符合 5.1 和 5.2 的要求;
b) 核查是否符合 5.3、5.4 和 5.5 的要求;

c) 核查是否采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对重要数据在存储过程中进行完整性保护，并验证存储数据完整性保护机制是否正确和有效。

6.4.7.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.4.7.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.4.7.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

6.4.8 不可否认性

6.4.8.1 测评指标

本单元测评指标如下：

——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(适用于第三级)；

——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(适用于第四级)。

6.4.8.2 测评对象

业务应用，以及提供不可否认性功能的密码产品等。

6.4.8.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见附录 B 和附录 C)：

a) 核查是否符合 5.1 和 5.2 的要求；

b) 核查是否符合 5.3、5.4 和 5.5 的要求；

c) 核查是否采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为和接收行为实现不可否认性，并验证不可否认性实现机制是否正确和有效。

6.4.8.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 6.4.8.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果 6.4.8.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7 管理测评要求

7.1 管理制度

7.1.1 密码应用安全管理制度

7.1.1.1 测评指标

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(适用于第一级到第四级)。

7.1.1.2 测评对象

密码应用安全管理制度类文档。

7.1.1.3 测评实施

核查各项安全管理制度是否包括密码人员管理、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。

7.1.1.4 结果判定

如果7.1.1.3测评实施内容均为是，则本单元的测评结果为符合；如果7.1.1.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.1.2 密钥管理规则

7.1.2.1 测评指标

应根据密码应用方案建立相应密钥管理规则(适用于第一级到第四级)。

7.1.2.2 测评对象

密码应用方案、密钥管理制度及策略类文档。

7.1.2.3 测评实施

核查是否有通过评估的密码应用方案，并核查是否根据密码应用方案建立相应密钥管理规则(例如，密钥管理制度及策略类文档中的密钥全生存周期的安全性保护相关内容)且对密钥管理规则进行评审，以及核查信息系统中密钥是否按照密钥管理规则进行生存周期的管理。

7.1.2.4 结果判定

如果7.1.2.3测评实施内容均为是，则本单元的测评结果为符合；如果7.1.2.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.1.3 操作规程

7.1.3.1 测评指标

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(适用于第二级到第四级)。

7.1.3.2 测评对象

操作规程类文档。

7.1.3.3 测评实施

核查是否对密码相关管理人员或操作人员的日常管理操作建立操作规程。

7.1.3.4 结果判定

如果7.1.3.3测评实施内容均为是，则本单元的测评结果为符合；如果7.1.3.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.1.4 安全管理制度

7.1.4.1 测评指标

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(适用于第三级到第四级)。

7.1.4.2 测评对象

密码应用安全管理制度类文档、操作规程类文档、记录表单类文档。

7.1.4.3 测评实施

核查是否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；对经论证和审定后存在不足或需要改进的密码应用安全管理制度和操作规程，核查是否具有修订记录。

7.1.4.4 结果判定

如果7.1.4.3测评实施内容均为是，则本单元的测评结果为符合；如果7.1.4.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.1.5 管理制度发布流程

7.1.5.1 测评指标

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(适用于第三级到第四级)。

7.1.5.2 测评对象

密码应用安全管理制度类文档、操作规程类文档、记录表单类文档。

7.1.5.3 测评实施

核查相关密码应用安全管理制度和操作规程是否具有相应明确的发布流程和版本控制。

7.1.5.4 结果判定

如果7.1.5.3测评实施内容均为是，则本单元的测评结果为符合；如果7.1.5.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.1.6 制度执行过程记录

7.1.6.1 测评指标

应具有密码应用操作规程的相关执行记录并妥善保存(适用于第三级到第四级)。

7.1.6.2 测评对象

密码应用安全管理制度类文档、记录表单类文档。

7.1.6.3 测评实施

核查是否具有密码应用操作规程执行过程中留存的相关执行记录文件。

7.1.6.4 结果判定

如果 7.1.6.3 测评实施内容均为是,则本单元的测评结果为符合;如果 7.1.6.3 测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.2 人员管理

7.2.1 密码相关法律法规和密码管理制度

7.2.1.1 测评指标

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(适用于第一级到第四级)。

7.2.1.2 测评对象

信息系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

7.2.1.3 测评实施

核查信息系统相关人员是否熟悉并遵守密码相关法律法规和密码应用安全管理制度。

7.2.1.4 结果判定

如果 7.2.1.3 测评实施内容均为是,则本单元的测评结果为符合;如果 7.2.1.3 测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.2.2 密码应用岗位责任制度

7.2.2.1 测评指标

本单元测评指标如下。

a) 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(适用于第二级)。

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(适用于第三级):

   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应与密钥管理员、密码操作员兼任;

4） 相关设备与系统的管理和使用账号不应多人共用。

c） 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（适用于第四级）：

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应与密钥管理员、密码操作员兼任；

4） 相关设备与系统的管理和使用账号不应多人共用；

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。

7.2.2.2 测评对象

密码应用安全管理制度类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等）。

7.2.2.3 测评实施

本单元测评实施如下。

a） 对于第二级的信息系统，核查是否建立了密码应用岗位责任制度，安全管理制度中是否明确了各岗位在安全系统中的职责和权限。

b） 对于第三级的信息系统，核查安全管理制度类文档是否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并定义岗位职责；核查是否对关键岗位建立多人共管机制，并确认密码安全审计员岗位人员是否不兼任密钥管理员、密码操作员等关键安全岗位；核查相关设备与系统的管理和使用账号是否有多人共用情况；离职人员及时删除其账号。

c） 对于第四级的信息系统，核查安全管理制度类文档是否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并定义岗位职责；核查是否对关键岗位建立多人共管机制，并确认密码安全审计员岗位人员是否不兼任密钥管理员、密码操作员等关键安全岗位；核查相关设备与系统的管理和使用账号是否有多人共用情况；离职人员及时删除其账号；核查密钥管理员、密码安全审计员和密码操作员是否由本机构的内部员工担任，是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录等。

7.2.2.4 结果判定

如果 7.2.2.3 相应等级的测评实施内容均为是，则本单元的测评结果为符合；如果 7.2.2.3 相应等级的测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.2.3 上岗人员培训制度

7.2.3.1 测评指标

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（适用于第二级到第四级）。

7.2.3.2 测评对象

密码应用安全管理制度类文档和记录表单类文档、系统相关人员（包括系统负责人、安全主管、密钥

管理员、密码安全审计员、密码操作员等)。

7.2.3.3 测评实施

核查安全教育和培训计划文档是否具有针对涉及密码的操作和管理的人员的培训计划;核查安全教育和培训记录是否有密码培训人员、密码培训内容、密码培训结果等的描述。

7.2.3.4 结果判定

如果 7.2.3.3 的测评实施内容均为是,则本单元的测评结果为符合;如果 7.2.3.3 测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.2.4 安全岗位考核

7.2.4.1 测评指标

应定期对密码应用安全岗位人员进行考核(适用于第三级到第四级)。

7.2.4.2 测评对象

密码应用安全管理制度类文档和记录表单类文档、系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

7.2.4.3 测评实施

核查安全管理制度文档是否包含具体的人员考核制度和惩戒措施;核查人员考核记录内容是否包括安全意识、密码操作管理技能及相关法律法规;核查记录表单类文档确认是否定期进行岗位人员考核。

7.2.4.4 结果判定

如果 7.2.4.3 测评实施内容均为是,则本单元的测评结果为符合;如果 7.2.4.3 测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.2.5 关键岗位人员保密制度

7.2.5.1 测评指标

本单元测评指标如下:

——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(适用于第一级);

——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(适用于第二级到第四级)。

7.2.5.2 测评对象

密码应用安全管理制度类文档和记录表单类文档、系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

7.2.5.3 测评实施

本单元测评实施如下:

a) 对于第一级的信息系统,核查人员离岗时是否具有及时终止其所有密码应用相关的访问权限、

操作权限的记录；

b） 对于第二级到第四级的信息系统，核查人员离岗的管理文档是否规定了关键岗位人员保密制度和调离制度等；核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。

7.2.5.4 结果判定

如果 7.2.5.3 相应等级的测评实施内容均为是，则本单元的测评结果为符合；如果 7.2.5.3 相应等级的测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.3 建设运行

7.3.1 密码应用方案

7.3.1.1 测评指标

应根据信息系统密码应用需求和依据密码相关标准，制定密码应用方案（适用于第一级到第四级）。

7.3.1.2 测评对象

密码应用方案。

7.3.1.3 测评实施

核查在信息系统规划阶段，是否依据信息系统密码应用需求和密码相关标准，制定密码应用方案，并核查方案是否通过评估。

7.3.1.4 结果判定

如果 7.3.1.3 测评实施内容均为是，则本单元的测评结果为符合；如果 7.3.1.3 测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.3.2 密钥安全管理策略

7.3.2.1 测评指标

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，各环节密钥管理检查要点参照附录 A（适用于第一级到第四级）。

7.3.2.2 测评对象

密码应用方案、密钥管理制度及策略类文档、密钥管理过程记录。

7.3.2.3 测评实施

本单元测评实施如下。

a） 核查是否有通过评估的密码应用方案；核查密钥管理制度及策略类文档是否确定系统设计的密钥种类、体系及其生存周期环节，是否与密码应用方案一致；如信息系统没有相应的密码应用方案，参照附录 A 核查密钥管理制度及策略类文档。

b） 核查相关密钥管理过程记录，核查是否按照密钥管理制度及策略类文档完成密钥管理。

7.3.2.4 结果判定

如果 7.3.2.3 测评实施内容均为是，则本单元的测评结果为符合；如果 7.3.2.3 测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.3.3 实施方案

7.3.3.1 测评指标

应按照应用方案实施建设（适用于第一级到第四级）。

7.3.3.2 测评对象

密码实施方案。

7.3.3.3 测评实施

核查是否有通过评估的密码应用方案，并核查是否按照密码应用方案，制定密码实施方案。

7.3.3.4 结果判定

如果 7.3.3.3 测评实施内容均为是，则本单元的测评结果为符合；如果 7.3.3.3 测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.3.4 投入运行前的密码应用安全性评估

7.3.4.1 测评指标

本单元测评指标如下：

——投入运行前可进行密码应用安全性评估（适用于第一级）；

——投入运行前宜进行密码应用安全性评估（适用于第二级）；

——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（适用于第三级到第四级）。

7.3.4.2 测评对象

密码应用安全性评估报告。

7.3.4.3 测评实施

本单元测评实施如下。

a) 对于第一级到第二级的信息系统，核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告。

b) 对于第三级到第四级的信息系统，核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告且系统通过评估。

7.3.4.4 结果判定

如果 7.3.4.3 相应等级的测评实施内容均为是，则本单元的测评结果为符合；如果 7.3.4.3 相应等级的测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.3.5 投入运行后的密码应用安全性评估

7.3.5.1 测评指标

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(适用于第三级到第四级)。

7.3.5.2 测评对象

密码应用安全管理制度、密码应用安全性评估报告、攻防对抗演习报告、整改文档。

7.3.5.3 测评实施

核查信息系统投入运行后，信息系统责任方是否严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并具有相应的密码应用安全性评估报告及攻防对抗演习报告；核查是否根据评估结果制定整改方案，并进行相应整改。

7.3.5.4 结果判定

如果 7.3.5.3 测评实施内容均为是，则本单元的测评结果为符合；如果 7.3.5.3 测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.4 应急处置

7.4.1 应急策略

7.4.1.1 测评指标

本单元测评指标如下：

——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(适用于第一级)；

——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(适用于第二级)；

——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(适用于第三级到第四级)。

7.4.1.2 测评对象

密码应用应急策略、应急处置记录类文档。

7.4.1.3 测评实施

本单元测评实施如下。

a) 对于第一级的信息系统，核查用户是否根据密码产品提供的安全策略处置密码应用安全事件。

b) 对于第二级的信息系统，核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审，应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行；如发生过密码应用安全事件，核查是否具有相应的处置记录。

c) 对于第三级到第四级的信息系统，核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审，应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行；如发生过密码应用安全事件，核查是否立即启动应急

处置措施并具有相应的处置记录。

7.4.1.4 结果判定

如果 7.4.1.3 相应等级的测评实施内容均为是，则本单元的测评结果为符合；如果 7.4.1.3 相应等级的测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.4.2 事件处置

7.4.2.1 测评指标

本单元测评指标如下：

——事件发生后，应及时向信息系统主管部门进行报告(适用于第三级)；

——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(适用于第四级)。

7.4.2.2 测评对象

密码应用应急策略类文档、安全事件报告。

7.4.2.3 测评实施

本单元测评实施如下：

a) 对于第三级的信息系统，核查密码应用安全事件发生后，是否及时向信息系统主管部门进行报告；

b) 对于第四级的信息系统，核查密码应用安全事件发生后，是否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。

7.4.2.4 结果判定

如果 7.4.2.3 相应等级的测评实施内容均为是，则本单元的测评结果为符合；如果 7.4.2.3 相应等级的测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.4.3 处置情况上报

7.4.3.1 测评指标

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(适用于第三级到第四级)。

7.4.3.2 测评对象

密码应用应急策略类文档、安全事件发生情况及处置情况报告。

7.4.3.3 测评实施

核查密码应用安全事件处置完成后，是否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，如事件处置完成后，向相关部门提交安全事件发生情况及处置情况报告。

7.4.3.4 结果判定

如果 7.4.3.3 测评实施内容均为是，则本单元的测评结果为符合；如果 7.4.3.3 测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8 整体测评要求

8.1 概述

整体测评从单元间、层面间等方面进行测评和综合安全分析。整体测评包括单元间测评和层面间测评。

单元间测评是指对同一技术层面或管理方面内的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全防护能力的影响。

层面间测评是指对不同技术层面或管理方面之间的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全防护能力的影响。

8.2 单元间测评

在单元测评完成后，应对单元测评结果中存在的不符合项和部分符合项进行单元间测评，重点分析信息系统中是否存在同一层面单元间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的密码安全防护能力是否缺失，如果经过综合分析单元测评中的不符合项和部分符合项未导致信息系统整体安全防护能力的缺失，则对该测评单元的测评结果予以调整。

8.3 层面间测评

在单元测评完成后，应对单元测评结果中存在的不符合项和部分符合项进行层面间测评，重点分析信息系统中是否存在不同层面单元间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的密码安全防护能力是否缺失，如果经过综合分析单元测评中的不符合项和部分符合项未导致信息系统整体安全防护能力的缺失，则对该测评单元的测评结果予以调整。

9 风险分析和评价

密码应用安全性评估报告应对整体测评之后单元测评结果中的不符合项和部分符合项进行风险分析和评价。

对单元测评结果中存在的不符合项和部分符合项，采用风险分析方法分析密码应用在合规性、正确性和有效性方面对应的安全问题被威胁利用的可能性和对信息系统造成的影响，综合评价这些不符合项和部分符合项对信息系统带来的不同程度的安全风险。

不符合项和部分符合项是否会给信息系统带来高安全风险的判定依据可参考其他相关标准或文件。对未满足密码应用的合规性、正确性、有效性且存在明显安全风险的情形，例如使用的密码技术不符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，应结合具体业务场景做出高安全风险判定。

10 测评结论

信息系统密码应用测评的最终输出是密码应用安全性评估报告，在报告中应描述以下环节的测评情况：各个测评单元的测评结果、整体测评结果、风险分析和评价结果，以及测评结论等。其中，测评结

论基于整体测评结果和风险分析结果综合给出，分为如下三种。

a) 符合：信息系统所有单元测评结果不存在不符合项和部分符合项。

b) 基本符合：信息系统单元测评结果中存在不符合项和部分符合项，与测评指标存在一定差距，但存在的不符合项和部分符合项未导致信息系统高安全风险。

c) 不符合：信息系统单元测评结果中存在不符合项和部分符合项，与测评指标存在较大差距，或存在的不符合项和部分符合项导致信息系统高安全风险。

附 录 A
（资料性）
密钥生存周期管理检查要点

A.1 概述

密钥管理对于保证密钥全生存周期的安全性至关重要，可以保证密钥（除公开密钥外）不被非授权的访问、使用、泄露、修改和替换，可以保证公开密钥不被非授权的修改和替换。在信息系统密码应用方案中，需明确信息系统的密钥生存周期管理。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。

A.2 密钥产生

密钥产生测评内容如下。

a） 检查目的

密钥是否在经商用密码认证机构认证的密码产品中产生，密钥协商算法是否经国家密码管理部门核准。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 确认密钥产生所使用的随机数发生器是否具有商用密码认证机构颁发的认证证书；

2） 确认密钥协商算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

3） 核实密钥产生功能的正确性和有效性，如随机数发生器的运行状态、所产生密钥的关联信息，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。

A.3 密钥分发

密钥分发测评内容如下。

a） 检查目的

密钥分发过程是否保证了密钥的机密性、完整性以及分发者、接收者身份的真实性等。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 确认信息系统内部采用何种密钥分发方式（离线分发方式、在线分发方式、混合分发方式）；

2） 确认密钥传递过程中信息系统使用了何种密码技术保证密钥的机密性、完整性与真实性，并核实采用密码技术的合规性、正确性和有效性。

A.4 密钥存储

密钥存储测评内容如下。

a) 检查目的

密钥(除公开密钥)存储过程是否保证了不被非授权的访问或篡改,公开密钥存储过程是否保证了不被非授权的篡改。

b) 检查对象

密钥、密钥管理制度及策略类文档,以及密钥存储涉及的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

1) 确认信息系统内部所有密钥(除公开密钥)是否均以密文形式进行存储,或者位于受保护的安全区域;

2) 确认密钥(除公开密钥)存储过程中信息系统使用了何种密码技术保证密钥的机密性(除公开密钥)、完整性,并核实采用密码技术的合规性、正确性和有效性;

3) 确认公开密钥存储过程中信息系统使用了何种密码技术保证公开密钥的完整性,并核实采用密码技术的合规性、正确性和有效性。

A.5 密钥使用

密钥使用测评内容如下。

a) 检查目的

所有密钥是否都有明确的用途且各类密钥是否均被正确地使用、管理。

b) 检查对象

密钥、密钥管理制度及策略类文档,以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

1) 确认信息系统内部是否具有严格的密钥使用管理机制,以及所有密钥是否有明确的用途并按用途被正确使用;

2) 确认信息系统是否具有鉴别公开密钥的真实性与完整性的认证机制,采用的公钥密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求;

3) 确认信息系统采用了何种安全措施来防止密钥泄露或替换,是否采用了密码算法以及算法是否符合相关法规和标准的要求,并核实当发生密钥泄露时,信息系统是否具备应急处理和响应措施;

4) 确认信息系统是否定期更换密钥,并核实密钥更换处理流程中是否采取有效措施保证密钥更换时的安全性。

A.6 密钥更新

密钥更新测评内容如下。

a) 检查目的

密钥是否根据相应的更新策略进行更新。

b) 检查对象

密钥、密钥管理制度及策略类文档,以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

确认信息系统是否具有密钥的更新策略,并核实当密钥超过使用期限、已泄露或存在泄露风险

时，是否根据相应的更新策略进行密钥更新。

A.7 密钥归档

密钥归档测评内容如下。

a） 检查目的

密钥归档过程是否保证了密钥的安全性和正确性，并生成了审计信息。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 确认信息系统内部密钥归档时是否采取有效的安全措施，以保证归档密钥的安全性和正确性；

2） 核实归档密钥是否仅用于解密被加密的历史信息或验证被签名的历史信息；

3） 确认密钥归档的审计信息是否包括归档的密钥、归档的时间等信息。

A.8 密钥撤销

密钥撤销测评内容如下。

a） 检查目的

公钥证书、对称密钥是否具备撤销机制。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 如信息系统内部使用公钥证书、对称密钥，则确认是否有公钥证书、对称密钥撤销机制和撤销机制的触发条件，并确认是否有效执行；

2） 核实撤销后的密钥是否已不具备使用效力。

A.9 密钥备份

密钥备份测评内容如下。

a） 检查目的

密钥备份过程是否保证了密钥的机密性和完整性，并生成了审计信息。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 如信息系统内部存在需要备份的密钥，则确认是否具有密钥备份机制并有效执行；

2） 确认密钥备份过程中，信息系统使用了何种密码技术保证备份密钥的机密性、完整性；

3） 确认是否包括备份主体、备份时间等密钥备份的审计信息。

A.10 密钥恢复

密钥恢复测评内容如下。

a） 检查目的

密钥是否具备恢复机制，并生成审计信息。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 确认信息系统内部是否具有密钥的恢复机制并有效执行；

2） 确认是否包括恢复主体、恢复时间等密钥恢复的审计信息。

A.11 密钥销毁

密钥销毁测评内容如下。

a） 检查目的

密钥是否具备销毁机制，销毁过程是否具备不可逆性。

b） 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c） 检查要点

1） 确认信息系统内部是否具有密钥的销毁机制并有效执行；

2） 核实密钥销毁过程和销毁方式，确认是否密钥销毁后无法被恢复。

附 录 B
（资料性）
典型密码功能测评技术

表 B.1 为第 6 章各测评单元中“测评实施”第三条“密码使用有效性”提供参考。典型密码功能包括真实性、机密性、完整性和不可否认性。其中，机密性分为传输机密性和存储机密性，完整性分为传输完整性和存储完整性。

表 B.1 典型密码功能测评技术

密码功能	对应测评单元	可能涉及的密码产品	测评实施要点	预期结果
传输机密性	6.2.3、6.3.2、6.4.4	IPSec/SSL VPN（互联网安全协议/安全套接层虚拟专用网）网关、密码机、智能密码钥匙等	1） 利用协议分析类工具，分析传输的重要数据或鉴别信息是否为密文、数据格式（如分组长度等）是否与信息系统实际使用的密码技术相符合； 2） 如果信息系统以外挂密码产品的形式实现传输机密性，如 VPN 网关、密码机、智能密码钥匙，见附录 C 中对这些密码产品应用的测评方法	1） 传输的重要数据和鉴别信息均为密文，数据格式（如分组长度等）与信息系统实际使用的密码技术相符合； 2） 实现传输机密性的密码产品在信息系统中被动正确使用且提供的传输机密性功能有效
存储机密性	6.4.5	密码机、智能密码钥匙等	1） 通过读取存储的重要数据，判断存储的数据是否为密文、数据格式（如分组长度等）是否与信息系统实际使用的密码技术相符合； 2） 如果信息系统以外挂密码产品的形式实现存储机密性，如密码机、智能密码钥匙，见附录 C 中对这些密码产品应用的测评方法	1） 存储的重要数据均为密文，数据格式（如分组长度等）与信息系统实际使用的密码技术相符合； 2） 实现存储机密性的外挂密码产品在信息系统中被正确使用且提供的存储机密性功能有效
传输完整性	6.2.2、6.3.2、6.4.6	IPSec/SSL VPN 网关、密码机、智能密码钥匙等	1） 利用协议分析类工具，分析被完整性保护的数据在传输时的数据格式（如签名长度、消息鉴别码的长度）是否与信息系统实际使用的密码技术相符合； 2） 如果采用数字签名技术进行完整性保护，可使用公钥对抓取的签名结果进行验证； 3） 如果信息系统以外挂密码产品的形式实现传输完整性，如 VPN 网关、密码机、智能密码钥匙，见附录 C 中对这些密码产品应用的测评方法	1） 被完整性保护的数据在传输时的数据格式（如签名长度、消息鉴别码的长度）与信息系统实际使用的密码技术相符合； 2） 使用签名技术进行完整性保护的，使用公钥对抓取的签名结果验证通过； 3） 实现传输完整性的外挂密码产品在信息系统中被正确使用且提供的传输完整性功能有效

表 B.1　典型密码功能测评技术（续）

密码功能	对应测评单元	可能涉及的密码产品	测评实施要点	预期结果
存储完整性	6.1.2、6.1.3、6.2.4、6.3.3、6.3.4、6.3.5、6.3.6、6.4.2、6.4.3、6.4.7	电子门禁系统、视频监控系统、密码机、智能密码钥匙等	1）通过读取存储的重要数据，判断被完整性保护的数据在存储时的数据格式（如签名长度、消息鉴别码的长度）是否与信息系统实际使用的密码技术相符合； 2）如果采用数字签名技术进行完整性保护，可使用公钥对存储的签名结果进行验证； 3）条件允许的情况下，可尝试对存储数据进行篡改（如修改消息鉴别码或数字签名结果），验证完整性保护措施的有效性； 4）如果信息系统以外挂密码产品的形式实现存储完整性保护，如电子门禁系统、视频监控系统、密码机、智能密码钥匙，见附录C中对这些密码产品应用的测评方法	1）被完整性保护的数据在存储时的数据格式（如签名长度、消息鉴别码的长度）与信息系统实际使用的密码技术相符合； 2）使用签名技术进行完整性保护时，使用公钥对存储的签名结果验证通过； 3）对存储数据进行篡改，完整性保护措施能够检测出存储数据的完整性受到破坏； 4）实现存储完整性的外挂密码产品在信息系统中被正确使用且提供的存储完整性功能有效
真实性	6.1.1、6.2.1、6.2.5、6.3.1、6.3.2、6.3.6、6.4.1	电子门禁系统、IPSec/SSL VPN网关、安全认证网关、动态令牌系统等	1）如果信息系统以外挂密码产品的形式实现对用户、设备的真实性鉴别，如电子门禁系统、VPN网关、安全认证网关、动态令牌系统等，则需要对密码产品应用情况进行测评，测评方法参考附录C中对这些密码产品应用的测评。 2）对于不能复用密码产品检测结果的，测评时还要查看实体鉴别机制是否符合GB/T 15843（所有部分）中的要求，特别是对于“挑战—响应”方式的鉴别协议，可以通过协议抓包分析，验证每次挑战值是否不同。 3）对于基于口令机制的鉴别过程，抓取鉴别过程的数据包，确认鉴别信息（如口令）未以明文形式传输；对于采用数字签名的鉴别过程，抓取鉴别过程的挑战值和签名结果，使用对应公钥验证签名结果的有效性；如采用了数字证书，见附录C中对证书认证系统应用的测评方法。 4）如果鉴别过程使用了数字证书，参考对证书认证系统应用的测评方法。如果鉴别未使用证书，密评人员要验证公钥或（对称）密钥与实体的绑定方式是否可靠，实际部署过程是否安全	1）实现对用户、设备的真实性鉴别的外挂密码产品在信息系统中被正确使用且提供的真实性性功能有效。 2）实体鉴别机制符合GB/T 15843（所有部分）中的要求。 3）对于口令鉴别方式，鉴别信息以非明文形式传输；对于使用数字签名进行鉴别，公钥验证签名结果通过。如果采用了数字证书，应符合证书认证系统相关要求。 4）公钥和（对称）密钥与实体的绑定方式可靠，部署过程安全

表 B.1　典型密码功能测评技术（续）

密码功能	对应测评单元	可能涉及的密码产品	测评实施要点	预期结果
不可否认性	6.4.8	智能密码钥匙、证书认证系统、电子签章系统等	1）　如果使用第三方电子认证服务，则应对密码服务资质进行核查，同时核查信息系统中是否配置了国家电子认证根 CA 证书并且在信息系统运行过程中是否对运营 CA 证书有效性进行了验证； 2）　使用相应的公钥对作为不可否认性证据的签名结果进行验证； 3）　如果使用智能密码钥匙、电子签章系统等密码产品实现不可否认性，见附录 C 中对这些密码产品应用的测评方法	1）　使用的第三方电子认证密码服务符合相关要求； 2）　使用相应公钥对不可否认性证据的签名结果的验证结果为通过； 3）　实现不可否认性的密码产品在信息系统中被正确使用且提供的不可否认性功能有效

附 录 C
（资料性）
典型密码产品应用测评技术

表 C.1 为附录 B 中涉及的密码产品应用的测评实施提供参考。

表 C.1 典型密码产品应用测评技术

产品类型	测评实施要点	预期结果
智能 IC 卡/智能密码钥匙	1) 进行错误尝试试验，验证在智能集成电路卡（智能 IC 卡）或智能密码钥匙未使用或错误使用（如使用他人的介质）时，相关密码应用过程（如鉴别）不能正常工作； 2) 条件允许情况下，在模拟的主机或抽选的主机上安装监控软件，用于对智能 IC 卡、智能密码钥匙的应用协议数据单元（APDU）指令进行抓取和分析，确认调用指令格式和内容符合预期（如口令和密钥是加密传输的）； 3) 如果智能 IC 卡或智能密码钥匙存储有数字证书，密评人员可以将数字证书导出后，对证书合规性进行检测，见本附录中对证书认证系统应用的测评方法； 4) 验证智能密码钥匙的口令长度和错误口令登录验证次数是否符合 GM/T 0027—2014 的要求。例如，智能密码钥匙的口令长度不小于 6 个字符，错误口令登录验证次数不大于 10 次	1) 智能 IC 卡或智能密码钥匙未使用或错误使用时，能够发现信息系统中相关密码应用（如身份鉴别）不能正常工作； 2) 信息系统调用智能 IC 卡、智能密码钥匙的指令格式和内容等符合预期，为信息系统提供了正确的密码功能； 3) 数字证书的格式和使用符合证书认证系统应用的有关要求； 4) 信息系统中使用的智能密码钥匙的口令长度和错误口令登录验证次数符合 GM/T 0027—2014 的要求
密码机	1) 利用协议分析类工具，抓取信息系统调用密码机的指令报文，验证其是否符合预期（如调用频率是否正常、调用指令是否正确）； 2) 管理员登录密码机查看相关配置，检查内部存储的密钥是否对应合规的密码算法，密码运算时是否使用合规的密码算法等； 3) 管理员登录密码机查看日志文件，根据与密钥管理、密码运算相关的日志记录，检查是否使用合规的密码算法等	1) 信息系统调用密码机的指令所对应的密码功能正确、调用次数符合预期； 2) 信息系统中使用的密码机，其内部存储的密钥对应合规的密码算法，并使用合规的密码算法进行密码运算； 3) 在相关的日志记录显示，信息系统使用的密码机采用了合规的密码算法

表 C.1　典型密码产品应用测评技术（续）

产品类型	测评实施要点	预期结果
VPN 产品和安全认证网关	1）利用端口扫描类工具，探测 IPSec VPN 和 SSL VPN 服务端所对应的端口服务是否开启。例如，IPSec VPN 服务对应的用户数据报协议（UDP）500、4500 端口，SSL VPN 服务常用的传输控制协议（TCP）443 端口（视产品而定）。	1）端口扫描显示信息系统中的 IPSec VPN 和 SSL VPN 服务端所对应的端口服务已经开启；
	2）利用协议分析类工具，抓取 IPSec 协议互联网密钥交换（IKE）阶段、SSL 协议握手阶段的数据报文，解析密码算法或密码套件标识是否属于已发布为标准的密码算法。例如，在 GB/T 36968—2018 中要求，IPSec 协议分组密码算法（SM4）标识为 129（由于历史原因，在部分早期产品中该值可能为 127），杂凑密码算法（SM3）标识为 20，椭圆曲线公钥密码算法（SM2）标识为 2；在 GM/T 0024—2014 中要求，SSL 协议中 ECDHE_SM4_SM3 套件标识为{0xe0，0x11}，ECC_SM4 _SM3 套件标识为{0xe0，0x13}，IBSDH_ SM4_SM3 套件标识为{0xe0，0x15}，IBC_SM4_SM3 套件标识为{0xe0，0x17}。	2）通过协议分析类工具分析，确认信息系统采用 IPSec、SSL 协议通信时使用的密码算法和密码套件标识属于已发布为标准的密码算法；
	3）利用协议分析类工具，抓取并解析 IPSec 协议 IKE 阶段、SSL 协议握手阶段传输的证书内容，判断证书是否合规，参见附录 D 中对证书认证系统应用的测评方法	3）证书格式和证书使用符合证书认证系统应用的有关要求
电子签章系统	1）检查电子印章的验证是否符合 GB/T 38540—2020 的要求，其中部分检测内容可以复用产品检测的结果；	1）通过复用产品检测结果等方式核实，信息系统中使用的电子签章系统，其电子印章的验证符合 GB/T 38540—2020 的要求；
	2）检查电子签章的生成和验证是否符合 GB/T 38540—2020 的要求，其中部分检测内容可以复用产品检测的结果	2）通过复用产品检测结果等方式核实，信息系统中使用的电子签章系统，其电子签章的生成和验证符合 GB/T 38540—2020 的要求
动态口令系统	1）判断动态令牌的 PIN 码保护机制是否满足 GB/T 38556—2020 的要求。例如，PIN 码长度不少于 6 位数字；如 PIN 码输入错误次数超过 5 次，则需至少等待 1 h 才可继续尝试；如 PIN 码输入超过最大尝试次数的情况超过 5 次，则令牌将被锁定，不可再使用。	1）信息系统中使用的动态令牌的 PIN 码保护机制满足 GB/T 38556—2020 的要求；
	2）尝试对动态口令进行重放，确认重放后的口令无法通过认证系统的验证。	2）对动态口令进行重放，重放后的口令无法通过认证系统的验证；
	3）核查种子密钥是否以密文形式导入到动态令牌和认证系统中	3）种子密钥以密文形式导入到动态令牌和认证系统中

表 C.1　典型密码产品应用测评技术（续）

产品类型	测评实施要点	预期结果
电子门禁系统	1）　尝试制作一些错误的门禁卡，验证这些卡无法打开门禁； 2）　利用发卡系统分发不同权限的卡，验证非授权的卡无法打开门禁； 3）　尝试复制门禁卡，验证无法进行有效复制	1）　错误的门禁卡无法打开门禁； 2）　不同权限的门禁卡仅能打开授权的门禁，非授权的卡无法打开门禁； 3）　门禁卡无法被复制使用
证书认证系统	1）　在信息系统中部署了证书认证系统产品，密评人员应核查证书认证系统产品及其涉及的密码产品是否具有商用密码认证机构颁发的认证证书； 2）　通过查看证书扩展项 KeyUsage 字段，确定证书类型（签名证书或加密证书），并验证证书及其相关私钥是否正确使用，在具体应用场景中签名证书只能用于数字签名，加密证书只能用于数据加密和密钥协商； 3）　通过数字证书格式合规性检测类工具，验证生成或使用的证书格式是否符合 GB/T 20518—2018 的有关要求； 4）　核查信息系统中是否配置了证书链并且在信息系统运行过程中是否对证书链有效性进行了验证	1）　信息系统使用的证书认证系统产品及其涉及的密码产品具有商用密码认证机构颁发的认证证书； 2）　信息系统中使用的数字证书及其私钥使用正确； 3）　生成和使用的证书格式符合 GB/T 20518—2018 的有关要求； 4）　信息系统在运行过程中对配置的证书链有效性进行了验证

参 考 文 献

[1] GB/T 15843.1(所有部分) 信息技术 安全技术 实体鉴别
[2] GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式
[3] GB/T 36968—2018 信息安全技术 IPSec VPN 技术规范
[4] GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范
[5] GB/T 38556—2020 信息安全技术 动态口令密码应用技术规范
[6] GM/T 0024—2014 SSL VPN 技术规范
[7] GM/T 0027—2014 智能密码钥匙技术规范
[8] 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
[9] GM/T 0037—2014 证书认证系统检测规范
[10] GM/T 0038—2014 证书认证密钥管理系统检测规范
[11] GM/T 0116—2021 信息系统密码应用测评过程指南