信息系统密码应用测评要求

中国密码学会密评联委会

二〇二〇年十二月

目　录

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不同等级密码应用的测评要求，从密码算法和密码技术合规性、密钥管理安全性方面，提出了第一级到第五级的密码应用通用测评要求；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、应用和数据安全等四个技术层面提出了第一级到第四级密码应用技术的测评要求；从管理制度、人员管理、建设运行和应急处置等四个管理方面提出了第一级到第四级密码应用管理的测评要求。

本文件适用于指导、规范信息系统密码应用在规划、建设、运行环节的商用密码应用安全性评估工作。

注：第五级密码应用测评要求只在本文件中描述通用测评要求。

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 37092 信息安全技术 密码模块安全要求

GB/T AAAAA 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 AAAAA和GM/Z 4001中界定的相关术语和定义，以及下列术语和定义适用于本文件。

3.1

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

是指商用密码应用安全性评估机构中从事商用密码应用安全性评估的人员，简称“密评人员”。

3.2

核查 examine

密评人员对测评对象进行观察、查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

4 概述

本文件根据GB/T AAAAA，将信息系统密码应用测评要求分为通用测评要求和密码应用测评要求。其中，第5章通用测评要求对“密码算法和密码技术合规性”和“密钥管理安全性”提出测评要求，适用于第一级到第五级的信息系统密码应用测评。第6章密码应用测评要求，对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技术层面提出了第一级到第四级密码应用技术

的测评要求，并对管理制度、人员管理、建设运行和应急处置四个方面提出了第一级到第四级密码应用管理的测评要求。

本文件第5章通用测评要求的内容不单独实施测评，也不单独体现在密码应用安全性评估报告的单元测评结果和整体测评结果中，仅供第6章密码应用测评要求的测评实施引用。资料性附录A密钥生存周期管理检查要点供第6.7.2节“制定密钥安全管理策略”的测评实施参考。资料性附录B给出了典型密码产品应用测评技术，资料性附录C给出了典型密码功能测评技术，供密评人员在对信息系统中具体使用的密码产品或应用的密码功能进行测评实施时参考。

本文件中的测评单元对应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。

a) 测评指标：来源于 GB/T AAAAA 中各级的要求项；
b) 测评对象：信息系统密码应用测评过程中不同测评方法作用的对象，包括相关配套密码产品、通用设备、人员、制度文档等；
c) 测评实施：针对某个测评指标，规定了信息系统密码应用的测评要点；
d) 结果判定：根据测评实施取得的证据，判定信息系统的密码应用是否满足某个测评指标要求的方法和原则。

若测评单元涉及两个及以上测评对象，则每个测评对象需要分别进行测评实施并结果判定。测评单元的结果由该单元涉及的所有测评对象的测评实施结果汇总得出。

密评人员在开展实际测评时，对于GB/T AAAAA中的不同安全保护等级的“可”“宜”“应”的条款，按照如下方法确定是否将其纳入测评范围。

——对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第6章相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。

——对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第6章相应的测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，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，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照第6章相应的测评指标要求进行测评和结果判定。

——对于“应”的条款，密评人员应按照第5章和第6章相应的测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

根据信息系统的密码应用方案和方案评审意见，若通过评估的密码应用方案中的要求，高于信息系统相对应的密码应用基本要求等级的指标要求，则应按照密码应用方案中的要求进行测评。例如，根据密码应用需求，对安全保护等级第三级的信息系统，选取了安全保护等级第四级信息系统的相关指标要求。对上述特殊情况进行测评实施的结论应体现在密码应用安全性评估报告中。

信息系统的商用密码应用测评的最终输出是密码应用安全性评估报告，在报告中应给出各个测评单元（见第 6 章）的测评结果、整体测评结果（见第 7 章），以及在进行风险分析和评价（见第 8 章）后给出的测评结论（见第 9 章）。其中，整体测评结果是以测评单元的判定结果为基础，经单元间、层面间测评相互弥补后得出的纠正结果；风险分析和评价是对整体测评结果中的不符合项和部分符合项，判断信息系统密码应用在合规性、正确性和有效性方面的不符合所产生的安全问题被威胁利用后对信息系

统造成影响的程度；测评结论是由综合得分以及风险分析和评价共同决定，表示信息系统达到相应密码等级保护要求的程度。

5 通用测评要求

5.1 密码算法和密码技术合规性

具体测评单元如下：

a) 测评指标

- 信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。（第一级到第五级）
- 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。（第一级到第五级）

b) 测评对象

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) 测评实施

了解系统使用的算法名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查密码算法是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意其使用的证明文件。核查系统所使用的密码技术是否以国家标准或行业标准形式发布。

d) 结果判定

本单元测评指标不单独判定符合性。

5.2 密钥管理安全性

具体测评单元如下：

a) 测评指标

- 信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。（第一级到第五级）
- 采用的密码产品，达到 GB/T 37092 一级及以上安全要求。（第二级）
- 采用的密码产品，达到 GB/T 37092 二级及以上安全要求。（第三级）
- 采用的密码产品，达到 GB/T 37092 三级及以上安全要求。（第四级）
- 采用的密码服务，符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。（第一级到第四级）

b) 测评对象

信息系统中的密钥体系，以及相应的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 测评实施

1) 核查信息系统中密钥体系中的密钥（除公钥外）是否不能被非授权的访问、使用、泄露、修改和替换，公钥是否不能被非授权的修改和替换；
2) 核查信息系统中用于密钥管理和密码计算的密码产品是否符合法律法规的相关要求，需依法接受检测认证的，核查是否经商用密码认证机构认证合格；了解密码产品的型号和版本等配置信息，核查密码产品是否符合 GB/T 37092 相应安全等级及以上安全要求，并核查密码产品的使用是否满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件；
3) 核查信息系统中用于密钥管理和密码计算的密码服务是否符合法律法规的相关要求，需依法接受检测认证的，核查是否经商用密码认证机构认证合格。

d) 结果判定

本单元测评指标不单独判定符合性。

6 密码应用测评要求

6.1 物理和环境安全

6.1.1 身份鉴别

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 核查电子门禁系统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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

采用密码技术保证视频监控音像记录数据的存储完整性。（第三级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

- 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。（第一级到第三级）
- 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。（第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 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（MAC）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（第一级到第三级）/双向身份鉴别（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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

采用密码技术保证通信过程中数据的完整性。（第一级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

采用密码技术保证通信过程中重要数据的机密性。（第一级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

采用密码技术保证网络边界访问控制信息的完整性。（第一级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第三级到第四级）

b) 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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 测评对象

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

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

远程管理设备时，采用密码技术建立安全的信息传输通道。（第三级到第四级）

b) 测评对象

通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供安全的信息传输通道的密码产品。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3) 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密码技术实现机制是否正确和有效。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

采用密码技术保证系统资源访问控制信息的完整性。（第一级到第四级）

b) 测评对象

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

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3） 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（MAC）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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

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。（第三级到第四级）

b） 测评对象

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

c） 测评实施

1） 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3） 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（MAC）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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

采用密码技术保证日志记录的完整性。（第一级到第四级）

b） 测评对象

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

c） 测评实施

1） 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3) 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（MAC）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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第三级到第四级）

b) 测评对象

通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、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。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 核查是否采用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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 测评对象

业务应用，以及提供身份鉴别功能的密码产品。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3） 核查应用系统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（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

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。（第一级到第四级）

b） 测评对象

业务应用，以及提供完整性保护功能的密码产品。

c） 测评实施

1） 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3） 核查信息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（MAC）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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

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。（第三级到第四级）

b） 测评对象

业务应用，以及提供完整性保护功能的密码产品。

c） 测评实施

1） 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3） 核查应用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（MAC）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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 测评对象

业务应用，以及提供机密性保护功能的密码产品。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 核查应用系统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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 测评对象

业务应用，以及提供机密性保护功能的密码产品。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；
2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；
3) 核查应用系统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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

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。（第一级到第四级）

b） 测评对象

业务应用，以及提供完整性保护功能的密码产品。

c） 测评实施

1） 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3） 核查应用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（MAC）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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

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。（第一级到第四级）

b） 测评对象

业务应用，以及提供完整性保护功能的密码产品。

c） 测评实施

1） 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2） 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3） 核查应用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（MAC）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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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

具体测评单元如下：

a） 测评指标

在可能涉及法律责任认定的应用中，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。（第三级到第四级）

b） 测评对象

业务应用，以及提供不可否认性功能的密码产品。

c) 测评实施

1) 核查是否符合第 5 章通用测评要求中“密码算法和密码技术合规性”的测评要求；

2) 核查是否符合第 5 章通用测评要求中“密钥管理安全性”的测评要求；

3) 核查应用系统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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 3）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。针对本测评单元，对该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。

6.5 管理制度

6.5.1 具备密码应用安全管理制度

具体测评单元如下：

a) 测评指标

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。（第一级到第四级）

b) 测评对象

安全管理制度类文档。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.5.2 密钥管理规则

具体测评单元如下：

a) 测评指标

根据密码应用方案建立相应密钥管理规则。（第一级到第四级）

b) 测评对象

密码应用方案、密钥管理制度及策略类文档。

c) 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（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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.5.3 建立操作规程

具体测评单元如下：

a) 测评指标

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。（第二级到第四级）

b) 测评对象

操作规程类文档。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.5.4 定期修订安全管理制度

具体测评单元如下：

a) 测评指标

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。（第三级到第四级）

b) 测评对象

安全管理制度类文档、操作规程类文档、记录表单类文档。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.5.5 明确管理制度发布流程

具体测评单元如下：

a) 测评指标

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。（第三级到第四级）

b) 测评对象

安全管理制度类文档、操作规程类文档、记录表单类文档。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.5.6 制度执行过程记录留存

具体测评单元如下：

a) 测评指标

具有密码应用操作规程的相关执行记录并妥善保存。（第三级到第四级）

b) 测评对象

安全管理制度类文档、记录表单类文档。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.6 人员管理

6.6.1 了解并遵守密码相关法律法规和密码管理制度

具体测评单元如下：

a) 测评指标

相关人员了解并遵守密码相关法律法规、密码应用安全管理制度。（第一级到第四级）

b) 测评对象

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

c) 测评实施

核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度。

d) 结果判定

针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.6.2 建立密码应用岗位责任制度

具体测评单元如下：

a) 测评指标

- 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。（第二级）
- 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：（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可与密钥管理员、密码操作员兼任；
4） 相关设备与系统的管理和使用账号不得多人共用。

- 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：（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可与密钥管理员、密码操作员兼任；
  4） 相关设备与系统的管理和使用账号不得多人共用；
  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。

b） 测评对象

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、密码审计员、密码操作员等）。

c） 测评实施

1） 第二级：

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。

2） 第三级：

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，并确认密钥管理员岗位人员是否不兼任密码审计员、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。

3） 第四级：

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，并确认密钥管理员岗位人员是否不兼任密码审计员、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；核查密钥管理员和密码操作员是否由本机构的正式人员担任，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。

d） 结果判定

针对单个测评对象，如果以上相应等级的测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.6.3 建立上岗人员培训制度

具体测评单元如下：

a) 测评指标

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。（第二级到第四级）

b) 测评对象

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、密码审计员、密码操作员等）。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.6.4 定期进行安全岗位人员考核

具体测评单元如下：

a) 测评指标

定期对密码应用安全岗位人员进行考核。（第三级到第四级）

b) 测评对象

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、密码审计员、密码操作员等）。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.6.5 建立关键岗位人员保密制度和调离制度

具体测评单元如下：

a) 测评指标

- 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。（第一级）
- 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。（第二级到第四级）

b) 测评对象

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、密码审计员、密码操作员等）。

c) 测评实施

1) 第一级：

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。

2） 第二级到第四级：

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。

d） 结果判定

针对单个测评对象，如果以上相应等级的测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.7 建设运行

6.7.1 制定密码应用方案

具体测评单元如下：

a） 测评指标

依据密码相关标准和密码应用需求，制定密码应用方案。（第一级到第四级）

b） 测评对象

密码应用方案。

c） 测评实施

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

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.7.2 制定密钥安全管理策略

具体测评单元如下：

a） 测评指标

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，各环节密钥管理要求参照 GB/T AAAAA 附录 B。（第一级到第四级）

b） 测评对象

密码应用方案、密钥管理制度及策略类文档。

c） 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，确定系统涉及的密钥种类、体系及其生存周期环节；若信息系统没有相应的密码应用方案，则参照附录 A 密钥生存周期管理检查要点核查密钥生存周期的各个环节是否符合要求。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.7.3 制定实施方案

具体测评单元如下：

a) 测评指标

按照应用方案实施建设。（第一级到第四级）

b) 测评对象

密码实施方案。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.7.4 投入运行前进行密码应用安全性评估

具体测评单元如下：

a) 测评指标

- 投入运行前进行密码应用安全性评估。（第一级到第二级）
- 投入运行前进行密码应用安全性评估，评估通过后系统方可正式运行。（第三级到第四级）

b) 测评对象

密码应用安全性评估报告、系统负责人。

c) 测评实施

1) 第一级到第二级

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。

2) 第三级到第四级

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。

d) 结果判定

针对单个测评对象，如果以上相应等级的测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.7.5 定期开展密码应用安全性评估及攻防对抗演习

具体测评单元如下：

a) 测评指标

在运行过程中，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，并根据评估结果进行整改。（第三级到第四级）

b) 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。

c） 测评实施

核查信息系统投入运行后，责任单位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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.8 应急处置

6.8.1 应急策略

具体测评单元如下：

a） 测评指标

- 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。（第一级）
- 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。（第二级）
- 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，立即启动应急处置措施，结合实际情况及时处置。（第三级到第四级）

b） 测评对象

密码应用应急处置方案、应急处置记录类文档。

c） 测评实施

1） 第一级

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。

2） 第二级

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；若发生过密码应用安全事件，核查是否具有相应的处置记录。

3） 第三级到第四级

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；若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。

d） 结果判定

针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.8.2 事件处置

具体测评单元如下：

a） 测评指标

- 事件发生后，及时向信息系统主管部门进行报告。（第三级）
- 事件发生后，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。（第四级）

b) 测评对象

密码应用应急处置方案、安全事件报告。

c) 测评实施

1) 第三级

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。

2) 第四级

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。

d) 结果判定

针对单个测评对象，如果以上相应等级的测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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。

6.8.3 向有关主管部门上报处置情况

具体测评单元如下：

a) 测评指标

事件处置完成后，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。（第三级到第四级）

b) 测评对象

密码应用应急处置方案、安全事件发生情况及处置情况报告。

c) 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。

d) 结果判定

针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该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 整体测评要求

7.1 概述

整体测评应从单元间、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安全层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密码应用防护能力的影响。

层面间测评是指对不同安全层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密码应用防护能力的影响。

7.2 单元间测评

在单元测评完成后，如果信息系统的某个测评单元的结果判定存在不符合或部分符合，应进行单元间测评，重点分析信息系统中是否存在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信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评中的不符合项或部分符合项不造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

7.3 层面间测评

在单元测评完成后，如果信息系统的某个测评单元的结果判定存在不符合或部分符合，应进行层面间测评，重点分析信息系统中是否存在层面间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评中的不符合项或部分符合项不造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

8 风险分析和评价

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

采用风险分析的方法，针对单元测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断信息系统密码应用在合规性、正确性和有效性方面的不符合所产生的安全问题被威胁利用后对信息系统造成影响的程度，以及受到威胁利用的资产自身价值，综合评价这些不符合项或部分符合项对信息系统造成的安全风险。

对于高风险的判定依据，可参考其他相关标准或文件，对未满足密码应用的正确性、有效性，或未使用经国家密码管理部门核准的密码技术且存在明显安全风险等措施，应结合具体业务场景做出高风险判定。

9 测评结论

密码应用安全性评估报告应给出信息系统的测评结论，确认信息系统达到相应等级保护要求的程度。

应结合整体测评和对单元测评结果的风险分析给出测评结论。

a) 符合：信息系统中未发现安全问题，测评结果中所有单元测评结果中部分符合和不符合项的统计结果全为 0，综合得分为 100 分；

b) 基本符合：信息系统中存在安全问题，部分符合和不符合项的统计结果不全为 0，但存在的安全问题不会导致信息系统面临高等级安全风险，且综合得分不低于阈值；

c) 不符合：信息系统中存在安全问题，部分符合项和不符合项的统计结果不全为 0，而且存在的安全问题会导致信息系统面临高等级安全风险，或综合得分低于阈值。

注：综合得分由各测评单元分数经整体测评修正后累加得到，可参考相关标准或文件了解详细得分规则。

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是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，可以保证公钥不被非授权的修改和替换。信息系统的应用与数据层面的密钥体系由业务系统根据密码应用需求在密码应用方案中明确。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。以下给出各个环节的检查要点建议，检查结果可用于密码应用测评结果评判参考。

A.2 密钥产生

a) 检查目的
密钥产生所使用的随机数发生器或密钥协商算法是否为经国家密码管理部门核准的。
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) 确认密钥是否在符合 GB/T 37092 的密码产品中产生；
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

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哪些密码技术对密钥进行处理以保护其机密性、完整性与真实性，并核实保护措施使用的正确性和有效性。

A.4 密钥存储

a) 检查目的
密钥（除公钥）存储过程是否保证了不被非授权的访问或篡改，公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) 确认系统内部所有密钥（除公钥）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（除公钥）存储过程中信息系统使用了哪些密码技术对密钥进行处理以保护其机密性（除公钥）、完整性，并核实保护措施使用的正确性和有效性；

3) 确认公钥存储过程中信息系统使用了哪些密码技术对公钥进行处理以保护其完整性，并核实保护措施使用的正确性和有效性。

A.5 密钥使用

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公钥认证机制，以鉴别公钥的真实性与完整性，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，是否使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漏时，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

a) 检查目的

密钥是否会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

1) 确认信息系统内部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，是否会根据相应的更新策略进行密钥更新。

A.7 密钥归档

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该密钥加密的历史信息或验证该密钥签名的历史信息；

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

a） 检查目的

公钥证书是否具备撤销机制。

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） 若信息系统内部使用公钥证书，则确认是否有公钥证书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

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） 若信息系统内部存在需要归档的密钥，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系统使用了哪些密码技术对密钥进行处理以保护其机密性、完整性；

3） 确认密钥备份的审计信息是否包括备份的主体、时间等信息。

A.10 密钥恢复

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） 确认系统内部是否具有密钥的恢复机制并有效执行；

2） 确认密钥恢复的审计信息是否包括恢复的主体、时间等信息。

A.11 密钥销毁

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）
典型密码产品应用测评技术

产品类型	测评实施	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（如 Bus Hound），用于对智能IC卡、智能密码钥匙的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，具体检测内容见对证书认证系统应用的测评； 4）验证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，相关密码应用能够检测出非正常使用； 2）智能IC卡、智能密码钥匙调用指令格式和内容符合预期； 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）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。
密码机	1）利用协议分析工具，抓取应用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，密码计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、密码计算相关的日志记录，检查是否使用合规的密码算法等。	1）应用系统调用密码机指令、次数等符合预期； 2）密码机内部存储的密钥对应合规的密码算法，使用合规的密码算法进行密码计算； 3）相关的日志记录显示使用合规的密码算法。
VPN 产品和安全认证网关	1）利用端口扫描工具，探测IPSec VPN和SSL VPN服务端所对应的端口服务是否开启，如IPSec VPN服务对应的UDP 500、4500端口，SSL VPN服务常用的TCP 443端口（视产品而定）； 2）利用通信协议分析工具，抓取IPSec协议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商用密码算法。IPSec协议SM4算法标识为129（由于历史原因，在部分早期产品中该值可能为127），SM3算法标识为20，SM2算法标识为2；SSL协议中ECDHE_SM4_SM3套件标识为{0xe0，0x11}，ECC_SM4 _SM3套件标识为 {0xe0，	1）端口扫描显示IPSec VPN和SSL VPN服务端所对应的端口服务已经开启； 2）通过通信协议分析工具分析，确认使用的密码算法和密码套件标识属于已发布为标准的商用密码算法； 3）证书的格式和使用符合证书认证系统应用的有关要求。

产品类型	测评实施	预期结果
	0x13}，IBSDH_ SM4_SM3套件标识为{0xe0,0x15}，IBC_SM4_SM3套件标识为{0xe0，0x17}； 3）利用协议分析工具，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，具体检测内容见对证书认证系统应用的测评。	
电子签章系统	1）检查电子印章的验证是否符合GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》的要求，其中部分检测内容可以复用产品检测的结果； 2）检查电子签章的生成和验证是否符合GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》的要求，其中部分检测内容可以复用产品检测的结果。	1）电子印章的验证符合GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》的要求； 2）电子签章的生成和验证符合GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》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以下要求：PIN 码长度不少于6位数字；若PIN码输入错误次数超过5次，则需至少等待1小时才可继续尝试；若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； 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； 3）核查种子密钥是以密文形式导入至动态令牌和认证系统中的。	1）动态令牌的PIN码保护机制满足要求； 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）种子密钥是以密文形式导入至动态令牌和认证系统中。
电子门禁系统	1）尝试发一些错误的门禁卡，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。	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。
证书认证系统	1）对信息系统内部署证书认证系统，密评人员可参考 GM/T 0037-2014《证书认证系统检测规范》和 GM/T 0038-2014《证书认证密钥管理系统检测规范》的要求进行测评； 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； 3）通过数字证书格式合规性检测工具，验证生成或使用的证书格式是否符合GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式规范》的有关要求。	1）证书及其私钥使用正确； 2）生成和使用的证书格式符合GB/T 20518-2018的有关要求。

附 录 C
（资料性）
典型密码功能测评技术

密码功能	测评实施	预期结果
传输机密性	1）利用协议分析工具，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）是否符合预期； 2）如果信息系统以外接密码产品的形式实现传输机密性，如VPN、密码机等，参考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）符合预期； 2）实现传输机密性的外接密码产品符合相应密码产品应用的要求。
存储机密性	1）通过读取存储的重要数据，判断存储的数据是否为密文，数据格式是否符合预期； 2）如果信息系统以外接密码产品的形式实现存储机密性，如密码机、加密存储系统、安全数据库等，参考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，数据格式符合预期； 2）实现存储机密性的外接密码产品符合相应密码产品应用的要求。
传输完整性	1）利用协议分析工具，分析受完整性保护的数据在传输时的数据格式（如签名长度、MAC长度）是否符合预期； 2）如果是使用数字签名技术进行完整性保护的，密评人员可以使用公钥对抓取的签名结果进行验证； 3）如果信息系统以外接密码产品的形式实现传输完整性，如VPN、密码机等，参考对这些密码产品应用的测评方法。	1）受完整性保护的数据在传输时的数据格式（如签名长度、MAC长度）符合预期； 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接密码产品符合相应密码产品应用的要求。
存储完整性	1）通过读取存储的重要数据，判断受完整性保护的数据在存储时的数据格式（如签名长度、MAC 长度）是否符合预期； 2）如果是使用数字签名技术进行完整性保护的，密评人员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，密评人员可尝试对存储数据进行篡改（如修改MAC或数字签名），验证完整性保护措施的有效性； 4）如果信息系统以外接密码产品的形式实现存储完整性保护，如密码机、智能密码钥匙，参考对这些密码产品应用的测评方法。	1）受完整性保护的数据在存储时的数据格式（如签名长度、MAC长度）符合预期； 2）使用签名技术进行完整性保护的，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接密码产品符合相应密码产品应用的要求。

密码功能	测评实施	预期结果
真实性	1）如果信息系统以外接密码产品的形式实现对用户、设备的真实性鉴别，如VPN、安全认证网关、智能密码钥匙、动态令牌等，参考对这些密码产品应用的测评方法； 2）对于不能复用密码产品检测结果的，还要查看实体鉴别协议是否符合GB/T 15843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）对于基于静态口令的鉴别过程，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； 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接密码产品符合相应密码产品应用的要求； 2）实体鉴别协议符合GB/T 15843中的要求； 3）静态口令的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，并且符合证书认证系统应用的相关要求； 4）公钥和（对称）密钥与实体的绑定方式可靠，部署过程安全。
不可否认性	1）如果使用第三方电子认证服务，则应对密码服务进行核查；如果信息系统中部署了证书认证系统，参考对证书认证系统应用的测评方法。 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）如果使用电子签章系统，参考对电子签章系统应用的测评方法。	1）使用的第三方电子认证密码服务或系统中部署的证书认证系统符合相关要求； 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）使用的电子签章系统符合电子签章系统应用的相关标准规范要求。

参 考 文 献

[1] GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》
[2] GM/T 0037-2014《证书认证系统检测规范》
[3] GM/T 0038-2014《证书认证密钥管理系统检测规范》
[4] GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式规范》
[5] GB/T 15843.2-2017《信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制》
[6] GB/T 15843.3-2016《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》
[7] GB/T 15843.4-2008《信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制》