



中华人民共和国密码行业标准

GM/T 0115—2021

信息系统密码应用测评要求

Testing and evaluation requirements for information
system cryptography application

2021-10-19 发布

2022-05-01 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 概述	1
5 通用测评要求	3
5.1 密码算法合规性	3
5.2 密码技术合规性	3
5.3 密码产品合规性	3
5.4 密码服务合规性	4
5.5 密钥管理安全性	4
6 密码应用技术和密码应用管理测评要求	4
6.1 物理和环境安全	4
6.2 网络和通信安全	6
6.3 设备和计算安全	8
6.4 应用和数据安全	11
6.5 管理制度	14
6.6 人员管理	17
6.7 建设运行	19
6.8 应急处置	21
7 整体测评要求	23
7.1 概述	23
7.2 单元间测评	23
7.3 层面间测评	23
8 风险分析和评价	23
9 测评结论	24
附录 A (资料性) 密钥生存周期管理检查要点	25
附录 B (资料性) 典型密码产品应用测评技术	29
附录 C (资料性) 典型密码功能测评技术	31
参考文献	33

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：国家密码管理局商用密码检测中心、中国科学院数据与通信保护研究教育中心、公安部三所（公安部信息安全等级保护评估中心）、上海交通大学、中国电子科技集团第十五研究所（信息产业信息安全测评中心）、国家信息技术安全研究中心、深圳市网安计算机安全检测技术有限公司、北京信息安全测评中心、山东道普测评技术有限公司。

本文件主要起草人：肖秋林、罗鹏、马原、陈天宇、郑昉昱、银鹰、张立花、吕娜、黎水林、刘健、杨宏志、吴冬宇、李晨旻、张晓溪。

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,从密码算法合规性、密码技术合规性、密码产品合规性、密码服务合规性以及密钥管理安全性等方面,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的密码应用技术测评要求;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的密码应用管理测评要求,并给出了整体测评、风险分析和评价、测评结论等测评环节的要求。

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 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 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

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

在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。

注: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 39786—2021,将信息系统密码应用测评要求分为通用测评要求、密码应用技术和密码应用管理测评要求。第 5 章用于指导第 6 章的实施,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。附录 A 为 5.5 的测评实施参考。附录 B 和附录 C 分别给出了典型密码产品应用测评技术和典型密码功能测评技术,供密评人员在対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 39786—2021 中各级的要求项,每条指标后面注明了指标对应的安全等级。
- 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,包括相关物理安防设施、通信信道、密码产品、通用设备、应用、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 39786—2021 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。

- a) 对于“可”的条款,由信息系统责任方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”。
- b) 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估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。
 - 1) 若纳入标准符合性测评范围,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。
 - 2) 若未纳入标准符合性测评范围,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。
- c) 对于“应”的条款,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。若根据信息系统的密码应用方案和方案评估意见,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估意见,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)、风险分析和评价结果(见第 8 章),以及在进行整体测评、风险分析和评价后给出的测评结论(见第 9 章)。其中,第 7 章整体测评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纠正结果;第 8 章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;第 9 章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等级保护要求的程度。

5 通用测评要求

5.1 密码算法合规性

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)。

b) 测评对象

信息系统中使用的密码产品、密码服务以及密码算法实现。

c) 测评实施

了解系统中所使用密码算法的名称、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使用的证明文件。

d) 结果判定

本单元测评指标不单独判定符合性。

5.2 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技术应符合密码相关国家标准和行业标准的要求(第一级到第五级)。

b) 测评对象

信息系统中的密码产品、密码服务以及密码技术实现。

c) 测评实施

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,或取得国家密码管理部门同意使用的证明文件。

d) 结果判定

本单元测评指标不单独判定符合性。

5.3 密码产品合规性

具体测评单元如下。

a) 测评指标

信息系统中使用的密码产品应符合法律法规和密码相关国家标准和行业标准的要求(第一级到第五级)。

若采用的密码产品依据密码模块相关标准,则应:

1) 达到密码模块安全等级一级及以上安全要求(第二级)。

2) 达到密码模块安全等级二级及以上安全要求(第三级)。

3) 达到密码模块安全等级三级及以上安全要求(第四级)。

b) 测评对象

信息系统中的密码产品。

c) 测评实施

了解信息系统中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,如其安全策略或使用手册说明

的部署条件。依据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。

d) 结果判定

本单元测评指标不单独判定符合性。

5.4 密码服务合规性

具体测评单元如下。

a) 测评指标

信息系统中使用的密码服务应符合法律法规和密码相关国家标准和行业标准的要求(第一级到第五级)。

b) 测评对象

信息系统中的密码服务。

c) 测评实施

核查信息系统中密码服务是否经商用密码认证机构认证合格或取得国家密码管理部门同意使用的证明文件。

d) 结果判定

本单元测评指标不单独判定符合性。

5.5 密钥管理安全性

具体测评单元如下。

a) 测评指标

1) 信息系统的密钥管理采用的密码产品、密码服务应符合法律法规和密码相关国家标准和行业标准的要求(第一级到第五级)。

2) 信息系统的密钥管理应符合密码相关国家标准和行业标准的要求(第一级到第五级)。

b) 测评对象

密钥管理采用的密码产品、密码服务及密钥管理实现。

c) 测评实施

1) 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。

2) 核查信息系统中密钥管理安全性实现技术是否正确有效。例如:非公开密钥是否不能被非授权的访问、使用、泄露、修改和替换,公开密钥是否不能被非授权的修改和替换。

d) 结果判定

本单元测评指标不单独判定符合性。

6 密码应用技术和密码应用管理测评要求

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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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c)的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

- 1) 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)。
- 2) 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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c)的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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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。

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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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、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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2；

2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5；

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的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 c) 的 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、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) 核查密码算法和密码技术是否符合 5.1 和 5.2；

2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5；

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 c) 的 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、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) 核查密码算法和密码技术是否符合 5.1 和 5.2;

2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;

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 c) 的 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、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) 核查密码算法和密码技术是否符合 5.1 和 5.2;

2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;

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 c) 的 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、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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;

- 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c)的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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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c)的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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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c)的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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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) 核查密码算法和密码技术是否符合 5.1 和 5.2;
- 2) 核查密码产品、密码服务和密钥管理是否符合 5.3、5.4 和 5.5;
- 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 c) 的 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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/105213003311011243>