信息系统密码应用高风险判定指引

中国密码学会密评联委会

二〇二〇年十二月

目　　录

信息系统密码应用高风险判定指引

1 范围

本文件依据GB/T AAAAA《信息安全技术 信息系统密码应用基本要求》有关条款，给出了信息系统密码应用过程中可能存在的高风险安全问题。

本文件适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

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 AAAAA 信息安全技术 信息系统密码应用基本要求

GM/T BBBB 信息系统密码应用测评要求

GM/Z 4001—2013 密码术语

3 术语和定义

GB/T AAAAA、GM/T BBBB和GM/Z 4001－2013中界定的术语和定义适用于本文件，以及下列术语和定义适用于本文件。

3.1

安全问题 security issues

资产中能被威胁所利用的弱点。

3.2

缓解措施 mitigation measure

是指可以降低威胁利用安全问题导致安全事件发生可能性的安全措施。

4 概述

本文件中判定内容由指标要求、适用范围、安全问题、可能的缓解措施和风险评价构成。其中，指标要求源自 GB/T AAAAA 的部分指标，对于本文件未覆盖的其他指标，仍需核查本文件第 5 章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题是否存在。

由于信息系统密码应用场景的复杂性，本文件无法涵盖密码应用的所有高风险安全问题，对于本文件未涉及但确实可能会对信息系统造成严重安全隐患的安全问题，应结合信息系统的实际情况对相关安全问题所引发的风险等级做出客观判断。在某些情况下，受限于具体场景的安全需求和各项条件，本文件给出的安全问题也可能不会导致信息系统面临较高安全风险，在信息系统密码应用的规划、建设、运行及测评时应结合具体场景进行合理判定。

5 通用要求

5.1 密码算法

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：所有级别信息系统。
c) 安全问题：
   1) 采用存在安全问题或安全强度不足的密码算法对重要数据进行保护，如MD5、DES、SHA-1、RSA（不足2048比特）等密码算法；
   2) 采用安全性未知的密码算法，如自行设计的密码算法、经认证的密码产品中未经安全性论证的密码算法。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

5.2 密码技术

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：所有级别信息系统。
c) 安全问题：
   1) 采用存在缺陷或有安全问题警示的密码技术，如SSH 1.0、SSL 2.0、SSL 3.0、TLS 1.0等；
   2) 采用安全性未知的密码技术，如未经安全性论证的自行设计的密码通信协议、经认证的密码产品中未经安全性论证的密码通信协议等。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

5.3 密码产品和密码服务

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：所有级别信息系统。
c) 安全问题：
   1) 采用自实现且未提供安全性证据的密码产品；
   2) 采用存在高危安全漏洞的密码产品，如存在Heartbleed漏洞的OpenSSL产品；
   3) 密码产品的使用不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；
   4) 选用的密码服务提供商不具有相关资质；
   5) 存在密钥管理相关安全问题（参见附录A）。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

6 物理和环境安全

6.1 身份鉴别

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：第二级及以上级别信息系统。
c) 安全问题：

1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
2) 未采用动态口令机制、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；
3) 针对人员身份真实性的密码技术实现机制不正确或无效。

d) 可能的缓解措施：
1) 基于生物识别技术（如指纹等）对进入人员进行身份鉴别；
2) 重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等。

e) 风险评价：
1) 若未采用密码技术对重要区域进入人员进行身份鉴别，但基于生物识别技术（如指纹等）保证了人员身份真实性，可酌情降低风险等级；
2) 若未采用密码技术对重要区域进入人员进行身份鉴别，或针对人员身份真实性的密码技术实现机制不正确或无效，但在重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等，可酌情降低风险等级。

7 网络和通信安全

7.1 身份鉴别

该部分包括以下内容：

a) 指标要求：采用密码技术对通信实体进行身份鉴别（第二级到第三级）/双向身份鉴别（第四级），保证通信实体身份的真实性。

b) 适用范围：第二级及以上级别信息系统。

c) 安全问题：
1) 存在第 5 章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
2) 信息系统与网络边界外建立网络通信信道时，未采用动态口令机制、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（第二级和第三级）/双向身份鉴别（第四级）；
3) 通信实体身份真实性实现机制不正确或无效；
4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：无。

e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

7.2 通信过程中重要数据的机密性

该部分包括以下内容：

a) 指标要求：采用密码技术保证通信过程中重要数据的机密性。

b) 适用范围：第二级及以上级别信息系统。

c) 安全问题：
1) 存在第 5 章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
2) 信息系统与网络边界外的通信实体建立网络通信信道时，未采用密码技术的加解密功能对通信过程中重要数据进行机密性保护；
3) 敏感信息或通信报文机密性实现机制不正确或无效；
4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：在“应用和数据安全”层面针对重要数据传输采用符合要求的密码技术进行机密性保护。

e) 风险评价：若未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，或机密性实现机制不正确或无效，但在“应用和数据安全”层面针对重要数据传输采用符合要求的密码技术进行机密性保护，可视为等效措施。

7.3 安全接入认证

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：第四级信息系统。
c) 安全问题：
   1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
   2) 未采用动态口令机制、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；
   3) 安全接入认证的实现机制不正确或无效；
   4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

8 设备和计算安全

8.1 身份鉴别

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：第二级及以上级别信息系统。
c) 安全问题：
   1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
   2) 未采用动态口令机制、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设备的用户进行身份鉴别；
   3) 用户身份真实性的密码技术实现机制不正确或无效。
d) 可能的缓解措施：基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性。
e) 风险评价：若未采用密码技术对登录设备的用户进行身份鉴别，或用户身份真实性的密码技术实现机制不正确或无效，但基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性，可酌情降低风险等级。

8.2 远程管理通道安全

该部分包括以下内容：

a) 指标要求：远程管理设备时，采用密码技术建立安全的信息传输通道。
b) 适用范围：第三级及以上级别信息系统。
c) 安全问题：
   1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
   2) 远程管理设备时，未采用密码技术建立安全的信息传输通道；
   3) 信息传输通道所采用密码技术实现机制不正确或无效；

4） 通过不可控网络环境进行远程管理，且鉴别数据以明文形式传输。

d) 可能的缓解措施：
   1) 搭建了与业务网络隔离的管理网络进行远程管理；
   2) 在“网络和通信安全”层面使用SSL VPN网关/IPSec VPN网关等建立集中管理通道，且使用的密码技术符合要求。

e) 风险评价：
   1) 若远程管理设备时未采用密码技术建立安全的信息传输通道，或远程管理信道所采用密码技术实现机制不正确或无效，但通过搭建与业务网络隔离的管理网络进行远程管理，可视为等效措施；
   2) 若在“网络和通信安全”层面使用SSL VPN网关/IPSec VPN网关等建立集中管理通道，且使用的密码技术符合要求，可视为等效措施。

9 应用和数据安全

9.1 身份鉴别

该部分包括以下内容：

a) 指标要求：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。

b) 适用范围：第二级及以上级别信息系统。

c) 安全问题：
   1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
   2) 未采用动态口令机制、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；
   3) 用户身份真实性的密码技术实现机制不正确或无效；
   4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性。

e) 风险评价：若未采用密码技术对登录用户进行身份鉴别，或用户身份真实性的密码技术实现机制不正确或无效，但基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性，可酌情降低风险等级。

9.2 重要数据传输机密性

该部分包括以下内容：

a) 指标要求：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。

b) 适用范围：第二级及以上级别信息系统。

c) 安全问题：
   1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；
   2) 未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；
   3) 重要数据传输机密性实现机制不正确或无效；
   4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：在“网络和通信安全”层面采用符合要求的密码技术保证重要数据在传输过程中的机密性。

e) 风险评价：若未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，或重要数据机密性实现机制不正确或无效，但在“网络和通信安全”层面采用符合要求的密码技术保证重要数据在传输过程中的机密性，可酌情降低风险等级。

9.3 重要数据存储机密性

该部分包括以下内容：

a) 指标要求：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。

b) 适用范围：第二级及以上级别信息系统。

c) 安全问题：

1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；

2) 未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；

3) 重要数据存储机密性实现机制不正确或无效；

4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：无。

e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

9.4 重要数据存储完整性

该部分包括以下内容：

a) 指标要求：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。

b) 适用范围：第二级及以上级别信息系统。

c) 安全问题：

1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；

2) 未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；

3) 重要数据存储完整性实现机制不正确或无效；

4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：应用系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份。

e) 风险评价：若未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，或重要数据存储完整性实现机制不正确或无效，但应用系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份，可酌情降低风险等级。

9.5 不可否认性

该部分包括以下内容：

a) 指标要求：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。

b) 适用范围：第三级及以上级别信息系统。

c) 安全问题：

1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；

2) 在可能涉及法律责任认定的应用中，未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；

3) 不可否认性的密码技术实现机制不正确或无效；

4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

d) 可能的缓解措施：无。

e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

10 密码应用管理要求

10.1 具备密码应用安全管理制度

该部分包括以下内容：

a) 指标要求：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。
b) 适用范围：第二级及以上级别信息系统。
c) 安全问题：未建立任何与密码应用安全管理活动相关的管理制度，或相关管理制度不适用于当前被测信息系统。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

10.2 制定密码应用方案

该部分包括以下内容：

a) 指标要求：依据密码相关标准和密码应用需求，制定密码应用方案。
b) 适用范围：第二级及以上级别信息系统。
c) 安全问题：对于新建信息系统，在规划阶段未制定密码应用方案或密码应用方案未通过评审。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

附 录 A
（资料性）
密钥管理安全问题

密钥管理对于保证密钥全生命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。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，以下给出可能会对密钥管理造成严重安全隐患的安全问题。

a) 密钥产生

密钥产生环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：

1) 未采用通过认证的随机数发生器生成密钥或密钥协商过程中的随机值，且无公开文献和证据证明随机数发生器的合理性和正确性；
2) 密钥在不可控的环境中生成；
3) 密钥协商之前或协商过程中没有验证对方身份真实性。

b) 密钥分发

密钥分发环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：

1) 使用没有访问控制机制的存储介质（如普通信封、普通U盘）等传输明文密钥，且管理制度无法保证密钥在分发过程中的安全性；
2) 密钥在不可控的环境中分发时，未使用密码技术保护密钥的机密性和完整性。

c) 密钥存储

密钥存储环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：

1) 密钥（除公钥外）以明文形式存储在不可控的环境中，且可以被非授权的访问、使用、泄露、修改和替换；
2) 公钥存储在不可控的环境中，且可以被非授权的修改和替换；
3) 用于加密密钥的口令以明文形式存储或复杂度小于10^12。

d) 密钥使用

密钥使用环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：

1) 在多个实体可以使用密钥的场景下，缺乏对密钥的使用控制机制；
2) 对称密钥使用过程中，由于使用不当导致密钥泄露；
3) 公钥与实体之间无任何关联关系；
4) 公钥与实体之间利用PKI技术进行关联，但使用前未验证公钥有效性或验证机制不完备；
5) 未按密钥用途正确使用。

e) 密钥更新

密钥更新环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：未建立密钥已泄露或存在泄露风险时的密钥更新机制。

f) 密钥销毁和撤销

密钥销毁和撤销环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：

1) 不具备密钥在应急或按需的密钥销毁/撤销的机制；
2) 未按照设定的机制进行密钥销毁/撤销。

g) 密钥恢复

密钥恢复环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：密钥在恢复使用时没有鉴别机制，可以被导入到其他系统中。