商用密码应用安全性评估
FAQ

中国密码学会密评联委会

首次发布日期：2021 年 12 月
最近更新日期：2021 年 12 月

目录

1.信息系统密码应用基本要求的等级 1
2.应、宜、可测评指标把握 1
3.经认证合格的密码产品中的密钥安全符合性判定 2
4.物理和环境安全层面的测评对象识别和确定 2
5.网络和通信安全层面的测评对象识别与确定 3
6.设备和计算安全层面的测评对象 5
7.设备和计算安全层面测评对象选取粒度 5
8.远程管理通道安全 6
9.合规密码产品身份鉴别、完整性相关指标的判定 7
10. 设备和计算安全层面的身份鉴别 7
11.应用和数据安全层面的测评对象识别与确定 8
12.访问控制信息的具体含义 8
13.缺少密码应用方案的合规性判定 9
14.商用密码产品认证证书过期的合规性判定 9
15.具有认证证书型号的商用密码产品对应的模块等级 9
16.有缓解措施的高风险判定 10
17.报告中对于高风险缓解措施的体现 10
18.双活机房的通信链路合规性判定 11
19.云平台测评的责任和范围 12
20.云平台和云上应用的测评方式和测评结论复用方式 12
21.面向公众等网站的测评 15
22.如何编写涉及应用和数据安全层面的测评内容报告 15

说明

本文件对商用密码应用安全性评估工作及相关标准中涉及的常见问题进行了整理和解答，以帮助相关人员更好的开展商用密码应用安全性评估工作。

本文件内容仅供参考，最终应以相关政策法规和标准规范为准。

编辑：张立花、肖秋林、郑昉昱、贾世杰、黎水林、王勇、范佳奇、刘健、刘军荣、冀利刚、杨宏志、李晨旸

审核：阎亚龙、马原、秦小龙、汪宗斌、罗鹏

本文件内容定期迭代更新发布，版本信息通过文件发布及更新日期记录表连续记录。

有关问题和建议，可发送邮件至mplwh@cacrnet.org.cn。

文件发布及更新日期记录表

首次发布日期	2021年12月
第一次更新日期	
第二次更新日期	
……	

1.信息系统密码应用基本要求的等级

- **背景：**

GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》对信息系统密码应用划分为自低向高的五个等级，参照GB/T 22239的等级保护对象应具备的基本安全保护能力要求，提出密码保障能力逐级增强的要求，用一、二、三、四、五表示。其中，从密码算法、密码技术、密码产品和密码服务的合规性方面，提出了第一级到第五级的密码应用通用要求，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、应用和数据安全四个技术层面提出了第一级到第四级的密码应用技术要求，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了第一级到第四级的密码应用管理要求。

- **问题：**

如何确定被测信息系统密码应用等级？

- **解答：**

GB/T 39786—2021中的密码应用等级一般由网络安全等级保护的级别确定。信息系统根据GB/T 22240—2020《信息安全技术 网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级，即等保定级为第一级的网络与信息系统应遵循GB/T 39786第一级密码应用基本要求，等保定级为第二级的网络与信息系统应遵循GB/T 39786第二级密码应用基本要求，以此类推。对于未完成网络安全等级保护定级的重要信息系统，其密码应用等级至少为第三级。

2.应、宜、可测评指标把握

- **背景：**

GB/T 39786对密码应用各项指标要求的力度，主要通过“应”“宜”“可”加以区分，具体实施时，需把握哪些是必须实现的、哪些是可以自行把握的。在“应”“宜”“可”三个指标中，“可”和“应”的含义明确，但“宜”含义，在GB/T 39786中有其特殊性。

- **问题：**

在密评实施中，如何理解和把握“宜”的指标要求？

- **解答：**

依据GM/T 0115《信息系统密码应用测评要求》，据信息系统的密码应用方案和方案评估报告/评审意见，决定是否将“宜”的指标要求纳入标准符合性测评范围，具体如下：

（1）若信息系统未编制密码应用方案或在方案中未对“宜”的指标要求做明确说明，则“宜”的指标要求纳入标准符合性测评范围。

（2）若信息系统编制了密码应用方案，且方案通过评估，方案中明确了不适用的“宜”的指标要求项，且有对应的风险控制措施说明的情况下。密评人员在测评时，应根据信息系统的密码应用方案和方案评估报告/评审意见，核实方案中的不适用指标要求项所采用的风险控制措施的适用条件，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方案中

所描述的风险控制措施是否一致，若满足适用条件，该测评指标为“不适用”；若不满足适用条件，则应纳入标准符合性测评范围，进行测评和结果判定。

3.经认证合格的密码产品中的密钥安全符合性判定

- **背景：**

GM/T 0115《信息系统密码应用测评要求》中，在通用测评要求中提出了“5.2密钥管理安全性”测评要求，其指标主要涉及密码产品/服务相关的内容。

- **问题：**

经认证合格的密码产品，《信息系统密码应用测评要求》中“5.2密钥管理安全性”测评是否可以直接判定为“符合”？

- **解答：**

不能直接判定为“符合”。信息系统采用经认证合格的密码产品仅仅是密钥管理安全性判定为“符合”的必要条件，还应当对以下内容进行核查：

(1) 该密码产品的安全级别是否满足GB/T 39786 相应等级的要求，如GB/T 39786第三级的信息系统应当采用满足GB/T 37092第二级及以上安全要求的密码产品；
(2) 由密码产品产生的密钥在该密码产品外部进行管理，是否进行了相应保护，如密钥在外部数据库中存储/备份/归档时是否进行了机密性和完整性保护；
(3) 该密码产品是否按照产品配套的安全策略文档进行部署和使用，信息系统的密钥管理制度是否能够保证该密码产品被正确地部署和使用等。

4.物理和环境安全层面的测评对象识别和确定

- **背景：**

GB/T 39786《信息安全技术 信息系统密码应用基本要求》在8.1节中要求“a)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；b)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；c)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”。相应的，GM/T 0115《信息系统密码应用测评要求》在“6.1物理和环境安全”中规定该安全层面的测评对象包括信息系统所在机房等重要区域及其电子门禁系统和视频监控系统。

- **问题：**

如何确定该层面的测评对象？对于系统部署在非被测系统单位管辖范围之内的情况，如运营商机房、云服务提供商机房、其他单位或部门管辖的机房等，在物理和环境安全层面应如何判定该指标的适用性？如何开展密评？

- **解答：**

物理和环境安全层面的测评对象为被测信息系统所在的物理机房，具体为物理机房的电子门禁系统和视频监控系统。

如果被测信息系统所在的物理机房采用多区域部署或被测信息系统重要资产分布在不同的物理机房中，那么针对该信息系统涉及的所有物理机房均应作为测评对象进行测评，密评人员需现场取证。

针对被测信息系统部署在被测系统单位管辖范围之外的情况，物理和环境安全层面仍然适用，即需要针对该安全层面进行测评。如果被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等通过了商用密码应用安全性评估，则可以复用商用密码应用安全性评估报告中“物理和环境安全”层面的相关测评结论；如果被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等未通过或未开展商用密码应用安全性评估，密评人员需现场取证，对于条件不允许的情况，可以要求IDC机房或云服务提供商机房等的运维方提供相关说明文件和证据以支撑测评结论。

5.网络和通信安全层面的测评对象识别与确定

- **背景：**

信息系统一般通过网络技术来实现与外界的互联互通，GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定了信息系统在网络和通信安全层面的密码应用技术要求，这些要求涉及到通信的主体（通信双方）、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、组件和产品。

- **问题：**

如何确定网络和通信安全层面的测评对象？

- **解答：**

网络和通信安全层面的测评对象主要是针对跨网络访问的通信信道，这里的跨网络访问指的是从不受保护的网络区域访问被测系统。

可以从通信主体和网络类型两个方面来确定网络和通信安全层面的测评对象：

(1) 网络类型：这里主要依据网络之间是否相对独立进行分类，如互联网、政务外网、企业专网等；

(2) 通信主体：指的是参与通信的各方，典型的如客户端与服务端。例如，PC机上运行的浏览器与服务器上运行的web服务系统，移动智能终端上运行的APP与服务器上运行的应用系统；也可以是服务端与服务端，例如，IPSec VPN与IPSec VPN之间。

【场景示例】

下面以一个具体场景来描述测评对象的确定过程。

在一个信息系统中，通常应用包括前台应用系统和后台管理系统；系统运行的网络环境通常包括互联网、政务外网和办公内网，其中，办公内网也属于政务外网。该信息系统网络通信情况描述如下。

(1) 用户可以从互联网、政务外网、办公内网，使用非国密浏览器或国密浏览器通过HTTPS协议访问前台应用系统；

(2) 管理员可以从办公内网或使用VPN客户端通过内网SSL VPN接入办公内网后，再使用国密浏览器通过HTTPS协议访问后台管理系统；

(3) 系统管理员可以从互联网先登录运维SSL VPN后，再通过堡垒机对服务器、密码产品等设备进行运维；

(4) 信息系统可以通过IPSec VPN调用外部的密码资源（例如政务外网的数据加密服务）。

针对此场景，根据通信主体，梳理出对应的网络类型，形成以下表格。

服务端 / 客户端	前台应用系统	后台管理系统	内网SSL VPN	运维SSL VPN	IPSec VPN
国密浏览器	互联网、政务外网	办公内网	-	-	-
非国密浏览器	互联网、政务外网	-	-	-	-
VPN客户端	-	-	政务外网	互联网	-
IPSec VPN	-	-	-	-	政务外网

根据上述表格描述，即可确定此信息系统网络和通信安全层面的测评对象。表中的每个元素表示通信主体可在某种网络类型下进行通信，例如表格第二行第二列表示：用户可在互联网和政务外网环境使用国密浏览器访问前台应用系统。由此可确定的两个测评对象为：互联网国密浏览器与前台应用系统之间的通信信道、政务外网国密浏览器与前台应用系统之间的通信信道。

根据以上的方法，此信息系统网络和通信安全层面的测评对象确定如下：

序号	测评对象	描述
1	互联网国密浏览器与前台应用系统之间的通信信道	用户从互联网使用国密浏览器通过HTTPS协议访问前台应用系统，密码应用主要测评HTTPS协议。
2	政务外网国密浏览器与前台应用系统之间的通信信道	用户从政务外网使用国密浏览器通过HTTPS协议访问前台应用系统，密码应用主要测评HTTPS协议。
3	互联网非国密浏览器与前台应用系统之间的通信信道	用户从互联网使用非国密浏览器通过HTTPS协议访问前台应用系统，密码应用主要测评HTTPS协议。
4	政务外网非国密浏览器与前台应用系统之间的通信信道	用户从政务外网使用非国密浏览器通过HTTPS协议访问前台应用系统，密码应用主要测评HTTPS协议。
5	政务外网VPN客户端与内网SSL VPN之间的通信信道	管理员用户从政务外网通过内网SSL VPN接入办公内网，密码应用主要测评SSL VPN协议。
6	办公内网国密浏览器与后台管理系统之间的通信信道	管理员从办公内网使用国密浏览器通过HTTPS协议访问后台管理系统，密码应用主要测评HTTPS协议。
7	互联网VPN客户端与运维SSL VPN之间的运维通信信道	系统管理员从互联网访问SSL VPN运维设备，密码应用主要测评SSL VPN协议。
8	政务外网IPSec VPN与IPSec VPN之间的通信信道	信息系统从政务外网通过IPSec VPN调用外部密码资源，密码应用主要测评IPSec VPN协议。

6.设备和计算安全层面的测评对象

- **背景：**

GM/T 0115《信息系统密码应用测评要求》在设备和计算层面的测评对象包括：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相应密码功能的密码产品。

- **问题：**

如何确定设备和计算安全层面的测评对象？

- **解答：**

设备和计算层面的测评对象主要包括通用服务器（如应用服务器、数据库服务器）、数据库管理系统、整机类和系统类的密码产品、堡垒机（当系统使用堡垒机用于对设备进行集中管理时，不涉及应用和数据安全层面）等。

交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为设备和计算安全层面的测评对象。需要注意若存在管理通道跨越边界的情况，需在网络和通信安全层面梳理一条远程管理数据传输通道作为测评对象。

建议在密评报告中，对设备和计算层面的测评对象进行分类整理和描述。至少分为密码产品/设备、具有密码功能的网络及安全设备、采用密码技术的其他产品、通用设备、不具有密码功能的网络及安全设备、虚拟设备和系统。

7.设备和计算安全层面测评对象选取粒度

- **背景：**

设备和计算安全层面的测评对象为通用服务器（如应用服务器、数据库服务器）、数据库管理系统、整机类和系统类密码产品、堡垒机等。

在一些较大型信息系统中，针对上述每一类测评对象，普遍均会部署多台设备（如部署多台服务器或者部署服务器集群，部署多台IPSec VPN以与不同的外界通信实体建立通信信道）。在这种情况下，在编写《商用密码应用安全性评估报告》时，设备和计算安全层面各个测评对象确定结果所选取的粒度会影响报告最后得分。

- **问题：**

如何确定设备和计算安全层面的各个测评对象选取的粒度？

- **解答：**

针对通用服务器和堡垒机，以“具有相同硬件、软件配置的设备”为粒度确定测评对象，即具有相同硬件配置（如生产厂商、型号等）和软件配置（如操作系统版本、中间件等）的服务器/堡垒机作为一个测评对象。以通用服务器为例，若某一信息系统部署了5台生产厂商为A、型号为B、操作系统版本为C的应用服务器，还部署了3台生产厂商为D、型号为E、操作系统版本为F的数据库服务器，则在《商用密码应用安全性评估报告》 “设备和计算安全测评对象确定结果”中，以“应用服务器（A-B- C）、数据库服务器（D-E-F）”作为测评对象。对通用服务器、堡垒机类的测评对象进行量化评估时，D/A/K均以各测评对象所包含的各个设备的实际应用情况的最低分值赋分。

针对整机类密码产品（如IPSec VPN网关、SSL VPN网关、安全认证网关、金融数据密码机、服务器密码机、签名验签服务器、时间戳服务器、云服务器密码机等）、系统类密码产品（如动态令牌认证系统、证书认证系统、证书认证密钥管理系统等），以“具有相同商用密码产品认证证书编号的密码产品”为粒度确定测评对象，即具有同一商用密码产品认证证书的密码产品作为一个测评对象。比如，某一信息系统部署了5台商用密码产品认证证书编号均为GMxxx的IPSec VPN，则在《商用密码应用安全性评估报告》“设备和计算安全测评对象确定结果”中，以“IPSec VPN（编号GMxxx）”作为测评对象。对密码产品类测评对象进行量化评估时，D/A/K均以各测评对象所包含的各个整机类的密码产品或系统类密码产品的实际应用情况的最低分值赋分。

8.远程管理通道安全

- **背景：**

GM/T 0115《信息系统密码应用测评要求》在网络和通信层面的测评对象为“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”，设备和计算层面“远程管理通道安全”测评项要求系统实现“远程管理设备时，采用密码技术建立安全的信息传输通道”。

- **问题：**

设备和计算安全层面“远程管理通道安全”测评项如何避免与网络和通信安全层面的测评对象重复测评，如何进行量化评估？

- **解答：**

以管理员在互联网通过SSL VPN接入系统内网后，登录堡垒机对设备进行远程管理为例，说明网络和通信安全层面和设备和计算安全层面“远程管理通道安全”测评单元关于远程管理数据传输通道测评内容的区别和量化评估方法。

对于网络和通信安全层面，只有当远程管理通道跨越网络边界时才将其作为该层面测评对象。如果只是在网络内部对设备进行管理，则不必将远程管理通道列为网络和通信安全层面的测评对象。针对在互联网访问SSL VPN接入内网后通过堡垒机对设备进行管理的情况，网络和通信安全层面仅需要测评由管理员在互联网访问VPN的过程，接入内网后访问堡垒机的过程体现在设备和计算安全层面。

对于设备和计算安全层面的“远程管理通道安全”测评单元，仅测评与测评对象直接相连的信息传输通道。测评对象为堡垒机时，无需测评管理员在互联网通过VPN接入系统内网的过程，因为该部分已在网络和通信安全层面体现，仅需测评接入内网后访问堡垒机的信息传输通道，如访问堡垒机管理应用时使用的HTTPS协议的密码应用情况；测评对象为通用服务器时，测评内容为通过堡垒机对设备进行管理的信息传输通道，如访问设备时使用的SSH协议的密码应用情况。

根据上述避免重复测评的方式，网络和通信安全层面将会根据SSL VPN提供的身份鉴别、通信数据机密性、完整性保护过程中的密码使用有效、密码算法/技术合规性、密钥管理情况进行量化评估；设备和计算层面“远程管理通道安全”测评项将根据接入内网后访问堡垒机，以及通过堡垒机管理设备时身份鉴别、通信数据机密性、完整性保护过程中的密码使用有效、密码算法/技术合规性、密钥管理情况进行量化评估。

考虑另外一种情况，若系统未部署SSL VPN，管理员可在互联网直接访问堡垒机对设备进行管理，在网络和通信安全层面、设备和计算安全层面“远程管理通道安全”测评单元均可将访问堡垒机的信息传输通道作为测评对象。

9.合规密码产品身份鉴别、完整性相关指标的判定

- **背景：**

通常情况下，信息系统责任单位通过部署密码产品以实现各项密码应用，信息系统责任单位只能通过密码产品的外部接口、系统配置界面等实现相应的密码应用，无法对密码产品内部的系统访问控制信息完整性、日志记录完整性、重要可执行程序完整性与来源真实性进行修改。

- **问题：**

合规密码产品的“身份鉴别”“系统资源访问控制信息完整性”“日志记录完整性”“重要可执行程序完整性、重要可执行程序来源真实性”等设备和计算安全层面的指标，应该如何测评？

- **解答：**

在确认密码产品具有合格的商用密码产品认证证书，且可以确定实际部署的密码产品与获认证产品一致的情况下，考虑到密码产品功能确定且自身安全防护能力较高，针对整机类密码产品的“系统资源访问控制信息完整性”“日志记录完整性”“重要可执行程序完整性、重要可执行程序来源真实性”这三个设备和计算安全层面的指标，可判定为符合。

但是，针对整机类密码产品的“身份鉴别”指标不能直接判定为符合，还需要进一步实地查看密码产品是否采用了密码技术（如智能IC卡、智能密码钥匙、动态口令等）对登录设备的用户等进行身份鉴别，从而保证用户身份的真实性。

10. 设备和计算安全层面的身份鉴别

- **背景：**

某些信息系统只能在本地进行设备登录运维，但是设备部署在相对安全的机房内部。由于设备改造难度较大，难以对设备的登录机制进行整改。

- **问题：**

仅进行本地运维的设备，如何针对设备和计算安全层面的“身份鉴别”和“远程管理通道安全”该如何进行测评和结果判定。

- **解答：**

测评机构需要首先核实设备确实仅进行本地运行，关闭了对外运维的接口。核实后，该测评对象的“远程管理通道安全”测评指标可作为不适用项，“身份鉴别”测评指标为适用项。

在对“身份鉴别”测评指标进行测评时，若本地运维均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，则该测评对象的测评结果为不符合。进一步地，对于不符合的情况，如果信息系统采用了必要的缓解手段（如《信息系统密码应用高风险判定指引》文件中所描述的采用基于特定设备或生物识别技术保证用

户身份的真实性），又或是将仅支持本地管理的被运维设备单独安置在具有良好安防措施的密闭区域（如机柜）内且仅有设备运维人员才有该区域的访问权限，可酌情降低风险等级。

11.应用和数据安全层面的测评对象识别与确定

- **背景：**

GM/T 0115《信息系统密码应用测评要求》在应用和数据层面的测评对象为“业务应用以及重要数据”。

- **问题：**

如何确定应用和数据安全层面的测评对象？

- **解答：**

应用和数据安全层面的测评对象应包含关键业务应用，具体参考通过专家评审后的密码应用方案设定的范围确定。如无密码应用方案，应根据网络安全等级保护定级报告描述的范围确定。关键业务应用一般情况下应包含被测系统的所有业务应用，关键业务应用中的关键数据一般包含但不限于以下数据：鉴别数据、重要业务数据、重要审计数据、个人敏感信息以及法律法规规定的其他重要数据类型。

12.访问控制信息的具体含义

- **背景：**

GB/T 39786《信息安全技术 信息系统密码应用基本要求》在网络和通信安全、设备和计算安全、应用和数据安全等层面均提出访问控制信息完整性保护需求，测评对象涉及网络通信实体、堡垒机、应用/数据库服务器、服务器密码机、签名验签服务器等设备，以及应用系统的访问控制信息（或称为访问控制列表）。

- **问题：**

网络和通信安全、设备和计算安全、应用和数据安全等层面提出的访问控制信息指什么？

- **解答：**

访问控制是在身份鉴别的基础上，控制主体对客体整体资源信息的访问控制管理。比如文件系统的访问控制（文件目录访问控制和系统访问控制）、文件属性访问控制、信息内容访问控制。访问控制的实现机制包含但不限于以下方式：目录表、访问控制列表、能力表、访问控制矩阵（访问控制列表、能力表组成的矩阵）、访问控制安全标签列表和权限位。

在网络和通信安全层面，要求为“采用密码技术保证网络边界访问控制信息的完整性”，强调的是网络边界。因此在该层面中，访问控制信息主要包括部署在网络边界的VPN中的访问控制列表、防火墙的访问控制列表、边界路由的访问控制列表等进行网络边界访问控制的信息。

在设备和计算安全中，要求为“采用密码技术保证系统资源访问控制信息的完整性”，强调的是系统资源。因此在该层面中，访问控制信息主要包括设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等。

在应用和数据安全中，要求为“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”，强调的是系统应用。因此在该层面中，访问控制信息主要包括应用系统的权限、标签等能够决定系统应用访问控制的措施等信息。

13.缺少密码应用方案的合规性判定

- **背景：**

GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》9.7节a)条款规定“应依据密码相关标准和密码应用需求，制定密码应用方案”，但很多已建信息系统并没有在系统规划时制定密码应用方案。

- **问题：**

在依据GB/T 39786—2021 9.7 a)条款密评时，密码应用方案该如何理解？

- **解答：**

对于已建信息系统，其密码应用方案并不追溯到系统最初规划时的方案，该信息系统根据相关标准、密码应用需求以及前期密评的整改建议，制定的密码应用改造方案可视为该系统的密码应用方案。后续，即可依据GM/T 0115《信息系统密码应用测评要求》的相关要求进行判定。需要说明的是，对于新建信息系统，除依据GM/T 0115进行符合性判定外，还应按照《信息系统密码应用高风险判定指引》进行风险评价。

14.商用密码产品认证证书过期的合规性判定

- **背景：**

在密评时，会发现商用密码产品型号证书过期的情况，即密评开展的时间在密码产品认证证书有效日期之后，而且产品厂商又提供不出更新后的认证证书。

- **问题：**

商用密码产品认证证书的有效期在密评时该如何把握？

- **解答：**

如无特殊情况和安全风险，密码产品的采购时间在商用密码认证证书在有效期内，则可判定为产品合规。此外，如果密评人员发现密码产品依据的相关密码标准已经失效或更新，则有义务告知信息系统单位相关情况，并建议其选用依据最新标准的密码产品。

15.具有认证证书型号的商用密码产品对应的模块等级

- **背景：**

在信息系统中密评时，使用的商用密码产品对应的认证证书分为两种，一种是认证证书上会标注有此密码产品对应的密码模块安全等级，一种是认证证书没有标注有密码产品对应的密码模块安全等级。

- **问题：**

未标注密码模块安全等级的商用密码产品在测评时如何判定？

- **解答：**

根据国家密码管理局和市场监管总局联合发布的《关于调整商用密码产品管理方式的公告》（第39号），自2020年7月1日起,已发放的《商用密码产品型号证书》自动失效，对有效期内的《商用密码产品型号证书》，持证单位可于2020年6月30日前，自愿申请转换国推商用密码产品认证证书，经认证机构审核符合认证要求后，直接换发认证证书，认证证书有效期与原《商用密码产品型号证书》有效期保持一致。

在实际测评时，未标注密码模块安全等级的产品可分以下两种情况：

对于换证的密码产品，因为其换发的认证证书上一律没有标注密码模块安全等级，此时需要密码厂商进一步提供换证前的商用密码产品型号证书，如果商用密码产品型号证书中标注了其符合的密码模块等级，则按此等级进行判定；否则，依据《商用密码应用安全性评估量化评估规则》按“密码产品等级不符合”进行判定。

对于新发认证证书的密码产品，市场监管总局和国家密码管理局发布的《商用密码产品认证目录》明确规定了密码模块标准适用的密码产品类型，其他产品（如安全芯片，密码系统类产品等）则不依据密码模块标准进行检测和认证。需要注意的是，虽然密码系统类产品（如电子门禁系统、CA/KM系统、电子签章系统等）不适用于密码模块标准，但作为系统组件的密码产品（如密码机、密码卡等）则适用于密码模块标准，也需要在密评时依据这些密码产品的密码模块安全等级进行判定。

16.有缓解措施的高风险判定

- **背景：**

《信息系统密码应用高风险判定指引》文件中，部分判定单元中提供了可能的缓解措施。

- **问题：**

如果被测系统使用了缓解措施，那么被测系统的风险等级、测评结论、分数是否发生改变？

- **解答：**

基于当前密码技术和产业发展现状，《信息系统密码应用高风险判定指引》部分判定单元中提供了可能的缓解措施，这样既体现了信息系统密码应用的重点和目标，同时也考虑了信息系统密码应用整改实际情况，能够较好地调动系统责任单位开展安全整改工作的积极性，从而有效推进信息系统密码应用工作。如果被测系统使用了相应的缓解措施，并通过评估确认缓解措施有效，原则上可以酌情降低其风险等级，但还应结合被测系统的实际情况进行分析，确认缓解措施能够有效抵御相关威胁，否则仍然维持其风险等级不变。如果因缓解措施导致风险等级发生改变，将可能造成测评结论发生改变，但测评分数仍保持不变。

17.报告中对于高风险缓解措施的体现

- **背景：**

在实际测评过程中，经常会发现系统存在《信息系统密码应用高风险判定指引》中描述的高风险安全问题，但是同时又采取了一定的缓解措施，那么如何在测评报告中体现高风险安全问题和缓解措施之间的关系呢？

- **问题：**

针对测评报告模板中高风险修正过程在哪个地方体现？

- **解答：**

如果测评报告问题涉及高风险判例中的问题场景，则需要在报告附录A中，按照实际评估结果进行填写，针对该测评项判定为不符合，但是在风险分析时针对该安全风险进行缓解措施说明。

【场景示例】

在密评报告（基于《商用密码应用安全性评估报告模板（2020版）》“第六章 风险分析”的表 6-1中的风险分析一列中将缓解高风险的理由进行描述，同时将风险等级进行重新评估。

表 6-1 风险分析

序号	安全层面	问题描述	关联威胁	风险分析	风险等级		
					高	中	低
1	物理和环境安全	XXXX 未使用密码技术对机房访问人员进行身份鉴别。	物理和环境	可能导致非法人员进入物理环境，对软硬件设备和数据进行破坏；但是现阶段机房使用了指纹识别技术对进入人员进行身份鉴别，能够在一定程度上降低该安全问题带来的风险。	0	1	0

18.双活机房的通信链路合规性判定

- **背景：**

信息系统一般通过网络技术来实现与外界的互联互通，网络和通信安全层面的测评对象，主要包括设备运维的通信信道、系统访问的通信信道等，那么针对双活机房之间通信的通信链路的测评如何处理？

- **问题：**

双活机房之间通信的通信链路，是否可作为网络和通信层面的一条通信信道？

- 解答：

因重要业务数据、重要个人信息等数据会在双活机房之间进行传输，双活机房之间的通信链路是否作为测评对象，需要根据被测系统实际情况进行判定：如果双活机房之间通过运营商专线进行数据通信，需参照GM/T 0115《信息系统密码应用测评要求》进行测评。

如果双活机房之间通信的通信链路是纯物理传输的裸光纤（需要被测方提供证明材料进行裸光纤判定），在对光纤物理防护上有严格的安全保护措施，能够完全保证物理线路安全，不存在安全隐患，则该通道无需作为网络和通信安全层面的测评对象。

19.云平台测评的责任和范围

- **背景：**

随着信息技术的发展，云计算已经被广泛应用。为降低系统成本，打通数据融合，越来越多的企业事业单位的系统选择部署在云上。云计算技术融合了软硬件资源，采用了虚拟化技术，主机边界和网络边界相对于传统数据中心来讲变得非常模糊，风险不但来自南北流量，还来自东西流量，部署在云平台上的系统，其安全风险也随之增加。实际测评中，经常会碰到云平台和云租户业务应用系统密码应用（以下称为“云上应用”）的密评，但是相对于传统的信息系统，云平台和云上应用的运营者一般不同。

- **问题：**

对运行在云平台上的云上应用进行密评时，特别是云平台和云上应用的运营者不同的情况下，如何界定两者的责任和范围。

- **解答：**

云平台系统的密码应用较为复杂，云平台系统的密码应用分为两个层面，一是云平台系统为满足自身安全需求所采用的密码技术，二是云租户通过调用云平台提供的密码服务为自身业务应用提供密码保障。因此，对运行在云平台上的云上应用进行密评时**原则上需要完成两部分测评工作：**

(1) 针对云平台自身密码应用的测评（以下简称“云平台测评”），该部分测评的责任主体为云平台的运营者。

(2) 针对云上应用系统密码应用的测评（以下简称“云上应用测评”），该部分测评的责任主体为云上应用的运营者。

同时，原则上：

(1) 云上应用系统所处的云平台通过密评（即获得“符合”或“基本符合”的结论）后，云上应用系统才能通过密评；

(2) 云上应用系统所处的云平台的安全级别应不低于云上应用系统。

20.云平台和云上应用的测评方式和测评结论复用方式

- **背景：**

云平台为云上应用提供了GB/T 39786中的物理和环境安全、网络和通信安全、设备和计算安全，甚至于应用和数据安全等层面在内的密码支撑。因此云上应用的部分测评结论需要依赖于云平台的测评结果。

- **问题：**

对运行在云平台上的云上应用进行密评时，那么如何分别对这两个系统进行分别测评，测评结论能够复用吗？

- **解答：**

云平台测评与一般信息系统基本一致，但由于云平台还需要为云上应用提供计算、存储、网络、密码等资源，还应关注云平台自身的密码应用以及对云租户提供的密码服务。对于云

平台自身而言，除了从物理和环境、网络和通信、设备和计算、应用和数据四个技术层面的密码应用进行测评外，还要兼顾云平台的服务模式，即要分别对云平台支持的每类服务模式（IaaS、PaaS、SaaS）进行密码应用测评，并关注对云租户提供的密码服务都有哪些，每台密码设备服务的边界。因此，在测评结论中还须包含“云平台密码支撑能力说明”，“云平台密码支撑能力说明”分为两类情况：

(1) **被完全评估的支撑能力：**指的是云平台中的**某些测评对象，这些测评对象**同时用于支撑云平台和云上应用，将同时作为云平台和云上应用的测评对象。比如，云平台运行所在的机房同时支撑了云平台和云上应用在物理和环境安全层面的密码应用安全，该机房既是云平台的测评对象 ，也是云上应用的测评对象。由于此时该支撑能力是云平台密码应用的一部分，它将在云平台密评时被“完全评估”，即该支撑能力有明确的测评结果（包括量化评估、风险评价等）。

(2) **被部分评估的支撑能力：**指的是云平台提供的**某些支撑服务，这些支撑服务**仅用于云上应用而不用于云平台，或者将服务于云平台和云上应用的不同测评对象。比如云平台的电子签章系统仅用于支撑了云上应用合同的抗抵赖保护，而不用于云平台本身；又比如云服务器密码机在进行数据存储保护时，面向的是云平台和云上应用的不同数据。由于这种情况下，该支撑能力必须结合云上应用的密码应用一起评估，因此无法在云平台测评时进行“完全评估”，只能进行“部分评估”，评估的内容包括：

1) 支撑能力相应的部分量化评估情况，包括《商用密码应用安全性量化评估规则》中定义的A和K的赋值和适用情况（即，在何种情况下可以取得相应量化评估分值；比如支撑能力提供了AES和SM4两种对称密码算法，在使用AES时，A为×；在使用SM4时，A为√）。

2) 支撑能力相应的风险评价和适用情况（即，在何种情况下可以取得相应风险评价结论）。

云上应用测评则与一般信息系统测评略有不同，其部分测评结论依赖于云平台测评的结果。测评过程中，需要根据云平台测评结论中的“云平台支撑能力说明”给定相应的测评结果。云上应用密评时，应重点关注应用本身在各个安全层面的密码应用情况。根据所使用支撑能力的不同，存在以下几种情况：

⑴ 云上应用被完全评估的支撑能力所支撑：此时，云上应用测评对象的测评结论完全被云平台对应对象的测评结论覆盖；**如果云平台已经通过密评（即获得“符合”或“基本符合”的结论）且安全等级不低于云上应用**，则云上应用测评对象的测评结论可以为“不适用”。

⑵ 云上应用被部分评估的支撑能力所支撑：此时，云上应用测评对象的测评结论需要结合“云平台支撑能力说明”对测评对象进行充分测评并给定结果。

⑶ 云上应用系统调用了非云平台提供的支撑能力：此时，云上应用测评对象的测评方式与一般信息系统类似，需要进行单独测评；**但是要重点关注该支撑能力与云平台、云上应用进行整合时是否安全，避免可能存在的安全风险。**比如，如果云上应用单独购置了一台服务器密码机进行数据存储保护，该服务器密码机直接接入云平台网络，但未进行必要的访问控制保护和安全隔离，导致了该服务器密码机被非授权调用或明文数据被非授权截取的风险，测评时应视情况进行结论的判定。

需要说明的是，实际测评过程中，上述规则可能存在以下无法适用或不能适用的情况：

(1) 云平台通过密评（即获得“符合”或“基本符合”的结论），但是其安全级别低于云上应用；此时，在对云上应用测评时，云平台的“云平台支撑能力说明”不再有效，仍需要对云平台相关的密码应用进行重新测评。

(2) 云平台未通过密评（没有开展密评，或未获得“符合”或“基本符合”的结论）；此时，在对云上应用测评时，仍需要对云平台相关的密码应用进行（重新）测评。

云平台支撑能力说明模版如下：

表 1　被完全评估的支撑能力概述

序号	安全层面	被完全评估的支撑能力	
		测评对象	所涉及的指标
1	物理和环境安全	XXX 机房	身份鉴别、电子门禁记录数据存储完整性
2		XXX 机房	
3		……	
4	网络和通信安全	XXX 通信信道	
5		XXX 通信信道	
6		……	
7	设备和计算安全	XXX 设备	
8		……	……
9	应用和数据安全	XXX 用户	
10		XXX 数据	
11		XXX 行为	
12		……	

表 1 被部分评估的支撑能力概述

序号	支撑能力名称	量化评估分值和适用条件				风险评估情况和适用条件	
		A	适用条件	K	适用条件	风险等级	适用情况
1	电子签章服务	√	当使用 SM3 和 SM2 算法进行电子签章时	√	（可以为“无”）	中、低	
		×	（可以为“无”）	×	（可以为“无”）	高	
2	时间戳服务	√		√		中、低	
		×		×		高	
3	服务器密码机	√		√		中、低	
		×		×		高	

21.面向公众等网站的测评

- **背景：**

政务信息公开网站、门户网站等面向公众的信息系统，具有内容可以公开、任何人都可以访问的特点，相应指标的测评需要进行额外的考量。

- **问题：**

面向公众、信息可公开的信息系统，需要重点关注哪些内容？

- **解答：**

首先，需要确定哪些人员可以访问该信息系统。除了面向公众用户之外，信息系统一般需要管理员对该系统进行管理，管理员的身份鉴别、传输通道安全等显然需要与一般信息系统一样，遵循相应的测评指标进行测评；

其次，对于公众用户而言，仍需要对网站进行身份鉴别（比如防止钓鱼网站），并对其内容的完整性进行保护；一般情况下还需要对用户访问网站产生的隐私数据（如访问情况、隐私行为等）进行保护，因此仍然需要测评公众用户相关的“网络和通信安全”层面“身份鉴别”“通信数据完整性”“通信过程中重要数据的机密性”等指标。

22.如何编写涉及应用和数据安全层面的测评内容报告

- **背景：**

在《商用密码应用安全性评估报告模板（2020版）》中，第3.3.2节“测评对象确定结果”、第4章“单元测评”和附录A.4“应用和数据安全”均涉及应用和数据安全层面的测评对象。此外，

第4章“单元测评”结果汇总，需要针对应用和数据安全层面关键数据的机密性和完整性保护情况进行说明和汇总。目前，针对该层面的内容报告编制形式多样，且存在各个密评机构对该层面的测评对象粒度把握尺度不一致的情况，对量化评估结果有一定的影响。

- **问题：**

如何编写密评报告中应用和数据安全层面的测评内容？

- **解答：**

信息系统业务应用的密码应用与其具体业务和安全需求密切相关，不同信息系统差异较为明显。在编制密评报告时，无论是较为简单的系统业务应用还是较为复杂的系统业务应用，在密评报告第3.3.2.1节的“表3-7应用和数据安全测评对象”和第4章节的“表4-4应用和数据安全测评结果汇总”中，可以都只列系统大的业务应用，而针对该层面身份鉴别、重要数据传输和存储保护的较为细粒度的测评对象，可以在第4章节“表4-4应用和数据安全测评结果汇总”下方，针对应用和数据安全层面身份鉴别情况、关键数据的机密性和完整性保护情况、不可否认性情况进行说明，以及附录中的测评结果记录中来体现。

下面以某信息化办公系统（第三级）为参考示例，给出该层面的报告编制案例。该信息化办公系统的业务应用包括OA办公系统、公文管理系统。其中，两个应用的用户均包括业务用户和管理员用户；OA办公系统和公文管理系统业务用户均有操作行为的不可否认性需求；OA办公系统的重要数据包括用户的身份鉴别信息、业务数据（仅有完整性需求）等，公文管理系统的重要数据包括用户的身份鉴别信息、业务数据（有机密性和完整性需求）等。

密评报告模板中第3.3.2.1节“表3-7应用和数据安全测评对象”可按照如下方式：

表 3-2 应用和数据安全测评对象

序号	测评对象	测评方式	说明
1	信息化办公系统应用	☑访谈 ☑文档审查 ☑实地查看 ☑配置检查 ☑工具测试	

相应的，在密评报告第4章节“单元测评”表4-4中可按照如下方式：

表 4-4 应用和数据安全测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）							
		身份鉴别	访问控制信息完整性	重要信息资源安全标记完整性	重要数据传输机密性	重要数据存储机密性	重要数据传输完整性	重要数据存储完整性	不可否认性
1	信息化办公系统应	部分符合	部分符合	不适用	部分符合	符合	部分符合	部分符合	部分符合

	用							
单元测评结果（符合/部分符合/不符合/不适用）	部分符合	部分符合	不适用	部分符合	符合	部分符合	部分符合	部分符合

针对应用和数据安全层面身份鉴别情况进行说明和汇总，如表 4-5-1 所示：

表 错误!文档中没有指定样式的文字。 **-5-1 应用和数据安全身份鉴别测评结果汇总**

序号	应用用户	身份鉴别
1	OA 办公系统管理员用户	部分符合
2	OA 办公系统业务用户	符合
3	公文管理系统管理员用户	符合
4	公文管理系统业务用户	符合
单元测评结果（符合/部分符合/不符合/不适用）		部分符合

针对应用和数据安全层面关键数据的机密性和完整性保护情况进行说明和汇总，如 4-5-2 所示：

表 4-3-2 应用和数据安全关键数据测评结果汇总

序号	关键数据	传输机密性	存储机密性	传输完整性	存储完整性
1	OA 办公系统管理员用户登录口令	不符合	符合	不符合	不符合
2	OA 办公系统业务用户登录口令	不符合	符合	不符合	不符合
3	OA 办公系统业务报表	不适用	不适用	符合	符合
4	OA 办公系统办公文件数据	不适用	不适用	符合	符合
5	OA 办公系统业务日志	不适用	不适用	符合	符合
6	公文管理系统管理员用户登录口令	符合	符合	不符合	不符合
7	公文管理系统业务用户登录口令	符合	符合	不符合	不符合
8	公文管理系统业务数据	符合	符合	不符合	符合
9	公文管理系统业务日志	符合	符合	不符合	符合
单元测评结果（符合/部分符合/不符合/不适用）		部分符合	符合	部分符合	部分符合

针对应用和数据安全层面不可否认性情况进行说明和汇总，如 4-5-3 所示：

表 4-5-3 应用和数据安全不可否认性测评结果汇总

序号	操作行为	不可否认性
1	OA 办公系统业务用户文件审批操作	部分符合
2	公文管理系统业务用户公文签发操作	符合
单元测评结果 （符合/部分符合/不符合/不适用）		部分符合

针对该系统示例的测评结果记录模板如下表 A-4 所示：

表 A-4 应用和数据安全测评结果记录

测评指标	测评对象	结果记录	量化指标				测评单元得分$\square_{\square\square}=\frac{\sum_{\square\le\square\le\square_{\square\square}}\square_{\square\square}\square_{\square\square\square}}{\square_{\square\square}}$
			密码使用有效 D	密码算法/技术合规性 A	密钥管理安全 K	测评对象评分 $S_{i,j,k}$	
身份鉴别	OA 办公系统管理员用户	略	✓	×	✓	0.5	略
	OA 办公系统业务用户	略	✓	✓	✓	1	
	公文管理系统管理员用户	略	✓	✓	✓	1	
	公文管理系统业务用户	略	✓	✓	✓	1	
访问控制信息完整性	OA 办公系统	略	✓	×	×	0.25	略
	公文管理系统	略	✓	✓	✓	1	
重要信息资源安全标记完整性	OA 办公系统	不适用				/	略
	公文管理系统	不适用				/	
重要数据传输机密性	OA 办公系统管理员 用户登录口令	略	×	×	×		略

	OA 办公系统业务用户登录口令	略	×	×	×		
	OA 办公系统业务报表	不适用				/	
	OA 办公系统办公文件数据	不适用				/	
	OA 办公系统业务日志	不适用				/	
	公文管理系统管理员用户登录口令	略	✓	✓	✓	1	
	公文管理系统业务用户登录口令	略	✓	✓	✓	1	
	公文管理系统业务数据	略	✓	✓	✓	1	
	公文管理系统业务日志	略	✓	✓	✓	1	
重要数据存储机密性	OA 办公系统管理员用户登录口令	略	✓	✓	✓	1	略
	OA 办公系统业务用户登录口令	略	✓	✓	✓	1	
	OA 办公系统业务报表	不适用					
	OA 办公系统办公文件数据	不适用					

	OA 办公系统业务日志	不适用					
	公文管理系统管理员用户登录口令	略	✓	✓	✓	1	
	公文管理系统业务用户登录口令	略	✓	✓	✓	1	
	公文管理系统业务数据	略	✓	✓	✓	1	
	公文管理系统业务日志	略	✓	✓	✓	1	
重要数据传输完整性	OA 办公系统管理员用户登录口令	略	×	×	×	0	略
	OA 办公系统业务用户登录口令	略	×	×	×	0	
	OA 办公系统业务报表	略	✓	✓	✓	1	
	OA 办公系统办公文件数据	略	✓	✓	✓	1	
	OA 办公系统业务日志	略	✓	✓	✓	1	
	公文管理系统管理员用户登录口令	略	×	×	×	0	
	公文管理系统业务用户登录口令	略	×	×	×	0	

	公文管理系统业务数据	略	×	×	×	0	
	公文管理系统业务日志	略	×	×	×	0	
重要数据存储完整性	OA 办公系统管理员用户登录口令	略	×	×	×	0	略
	OA 办公系统业务用户登录口令	略	×	×	×	0	
	OA 办公系统业务报表	略	✓	✓	✓	1	
	OA 办公系统办公文件数据	略	✓	✓	✓	1	
	OA 办公系统业务日志	略	✓	✓	✓	1	
	公文管理系统管理员用户登录口令	略	×	×	×	0	
	公文管理系统业务用户登录口令	略	×	×	×	0	
	公文管理系统业务数据	略	✓	✓	✓	1	
	公文管理系统业务日志	略	✓	✓	✓	1	
不可否认性	OA 办公系统业务用户文件审批操作	略	✓	×	✓	0.5	略

	公文管理系统业务用户公文签发操作	略	✓	✓	✓	1	