

# 商用密码应用安全性评估

## FAQ

### （第四版）

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：2026 年 3 月

# 目 录

前 言.....	I
<b>第四版与第三版 FAQ 对照情况表.....</b>	<b>II</b>
一、通用类.....	1
1. 信息系统密码应用基本要求的等级 .....	1
2. 具有认证证书的商用密码产品对应的模块等级.....	2
3. 经认证合格的密码产品的产品合规性、密钥安全符合性的判定要点.....	3
4. 通过代码实现数据机密性、完整性保护的判定方法.....	6
5. 组合密码算法的量化评估和风险判定.....	7
6. 如何开展分期规划、改造的信息系统的密码应用安全性评估.....	8
7. 已有通过评估的密码应用方案，在实际密评时的注意事项.....	9
8. 自建 CA 签发数字证书的合规性判定要点.....	9
9. 对于被测方没有改造和管理权限的接口进行密评的注意事项.....	10
二、密码应用技术类.....	11
<b>（一）物理和环境安全.....</b>	<b>11</b>
10. 物理和环境安全层面的测评对象识别和确定.....	11
11. 电子门禁记录数据存储完整性测评时的注意事项.....	13
<b>（二）网络和通信安全.....</b>	<b>14</b>
12. 网络和通信安全层面的测评对象识别与确定.....	14
13. 网络和通信安全层面的身份鉴别等指标.....	20
14. 网络层安全接入认证和身份鉴别指标的差别.....	21
<b>（三）设备和计算安全.....</b>	<b>22</b>
15. 设备和计算安全层面的测评对象识别与确定.....	22
16. 设备和计算安全层面测评对象选取粒度.....	23
17. 设备和计算安全层面的身份鉴别.....	24
18. 远程管理通道安全的测评要点 .....	26
19. 合规密码产品的设备层身份鉴别、完整性相关指标的判定.....	27
<b>（四）应用和数据安全.....</b>	<b>28</b>

20. 应用和数据安全层面的测评对象识别与确定.....	28
21. 应用和数据安全层面的身份鉴别.....	30
22. 重要数据机密性、完整性保护的实现方法问题.....	31
23. 应用和数据安全层面的存储机密性问题.....	33
<b>(五) 综合.....</b>	<b>34</b>
24. 访问控制信息的具体含义 .....	34
25. 跨网络调用密码资源实现相应密码功能的测评要点.....	36
<b>三、密码应用管理类.....</b>	<b>37</b>
26. 缺少密码应用方案的合规性判定.....	37
27. 投入运行前未进行密码应用安全性评估的合规性判定.....	37
28. 定期开展密码应用安全性评估及攻防对抗演习指标的合规性判定.....	38
29. 应急处置指标的合规性判定 .....	39
<b>四、整体测评类.....</b>	<b>40</b>
30. 测评对象间的弥补场景 .....	40
<b>五、量化评估类.....</b>	<b>41</b>
31. 《商用密码应用安全性评估量化评估规则（2023 版）》中，密码使用有效性 D 项的判定 .....	41
<b>六、风险判定类.....</b>	<b>42</b>
32. 有缓解措施的高风险判定 .....	42
33. 应用层身份鉴别是否可以缓解网络层身份鉴别的高风险.....	43
34. 如何理解高风险判定指引中的“适用时” .....	45
35. 不涉及高风险的指标使用了高风险算法、技术或产品进行保护时，如何判定风险 .....	45
<b>七、特殊场景类.....</b>	<b>46</b>
36. 云平台测评的责任和范围 .....	46
37. 云平台和云上应用的测评方式和测评结论复用方式.....	47
38. 面向公众等网站的测评 .....	52
39. 特殊系统的测评对象选取 .....	52
40. 如何开展信息系统密码应用成熟度极低情况下的密码应用管理测评.....	53
41. 特定行业或具有特殊密码应用需求的信息系统测评.....	54

## 前 言

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,以帮助密码应用以及商用密码应用安全性评估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。

编辑组:

第一版: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、李晨昉;

第二版:李智虎、王洋、朱凌、李海滨、高岩、李海涛、高锐、唐启楠、张腾标、李艳俊、陈爽、刘焯、佟鑫、管彩霞;

第三版:陈天宇、刘军荣、翟峰、秦琦、吕娜、郑峥、王正临、苏欧煜、张晓溪、朱凌、江寰、亢康、杨龙、佟鑫、李昊宸、陈爽、姚莹、王海涛、史汝辉、宋松、刘焯、卢秋如、邓福彪、薛涛。

第四版:张立花、李智虎、苏欧煜、王微、王建峰、陈小庆、刘焯、赵雨雨、张晓溪、唐启楠、吴栋、牛莹姣、刘琛、卢秋如、宋兴博、刘芝影、王海涛、李昊宸、谢孟凯。

审核组:刘平、秦小龙、罗鹏、阎亚龙、汪宗斌、马原、刘尚焱。

本文件内容不定期迭代更新发布。

有关问题和建议,可发送邮箱至 [mplwh@cacnet.org.cn](mailto:mplwh@cacnet.org.cn)

第四版与第三版 FAQ 对照情况表

序号	章节分类	第四版			第三版		
		章节名称	具体问题	备注	章节名称	具体问题	备注
1	一、通用类				2.应、宜、可测评指标把握	问题：在密评实施中，如何理解和把握“宜”的指标要求？	删除
2		2.具有认证证书的商用密码产品对应的模块等级	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？	根据《关于调整商用密码检测认证业务实施的公告》对解答进行补充	3.具有认证证书的商用密码产品对应的模块等级	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？	
3			3.2 问题：有些类型的密码产品部署模式为客户端与服务端共同作用，实现密码技术的应用。例如，VPN 等密码产品存在客户端和服务端的情况，在测评时应如何判断实际部署中涉及客户端的密码产品的合规性？	删除掉原解答中的下列表述：“或高于送检版本（版本迭代升级原因仅为 bug 修订，必要时需厂商提供变更说明）。”		4.2 问题：有些类型的密码产品部署模式为客户端与服务端共同作用，实现密码技术的应用。例如，VPN 等密码产品存在客户端和服务端的情况，在测评时应如何判断实际部署中涉及客户端的密码产品的合规性？	
4		3.经认证合格的密码产品的产品合规性、密钥安全符合性的判定要点	3.3 问题：如何确定密码产品的密码功能边界，例如，签名验签服务器实现了加解密功能，在测评时如何判定其合规性？	新增接口遵循 GM/T0020-2023《证书应用综合服务接口规范》标准的要求。	4.经认证合格的密码产品的产品合规性、密钥安全符合性的判定要点	4.3 问题：如何确定密码产品的密码功能边界，例如，签名验签服务器实现了加解密功能，在测评时如何判定其合规性？	
5			3.4 问题：经认证合格的密码产品，GB/T43206-2023《信息安全技术信息系统密码应用测评要求》中“5.5 密钥管理”测评是否可以直接判定为“符合”？	完善下列文字到回答中“如果被测系统无密码应用方案或系统密钥管理机制与方案不一致”		4.4 问题：经认证合格的密码产品，《信息安全技术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”？	
6		8.自建 CA 签发数字证书的合规性判定要点	问题：企业通过自建 CA 系统为信息系统签发用于加密通信和身份认证的数字证书，是否合规？	新增			

7		9.对于被测方没有改造和管理权限的接口进行密评的注意事项	问题：是否可以因为无改造和管理权限、责任方不在本系统范围等原因将这类互联互通论证为不适用？	新增			
8	二、密码应用技术类	12.网络和通信安全层面的测评对象识别与确定	12.2 问题：当被测系统使用第三方电子认证服务机构提供的认证服务完成系统功能时，被测系统与第三方电子认证服务相关系统之间的通信信道是否需要纳入测评范围？	补充完善答案，考虑访问CA本身的安全机制带来的影响以及证书数据机密性保护的必要性	11.网络和通信安全层面的测评对象识别与确定	11.2 问题：当被测系统使用第三方电子认证服务机构提供的认证服务完成系统功能时，被测系统与第三方电子认证服务相关系统之间的通信信道是否需要纳入测评范围？	
9			12.4 问题：针对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？	补充裸光纤的分类和判定建议		11.4 问题：针对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？	
10			12.6 问题：如果服务端同时支持国外和国密算法，如何选择该通道的测评对象？	新增			
11		13.网络和通信安全层面的身份鉴别	13.1 问题：采用合规的SSLVPN安全网关建立TLCP连接，但客户端采用的浏览器（插件）或客户端软件未获得商用密码产品认证证书，此时网络和通信安全层面的“身份鉴别”指标该如何进行判定？	新增	12.网络和通信安全层面的身份鉴别	问题：采用合规的SSLVPN安全网关，但安全通道使用安全强度足够高的国外密码算法套件，且客户端采用通用浏览器，此时网络和通信安全层面的“身份鉴别”指标该如何进行量化评估？	删除
12			13.2 问题：当用户使用“合规”的SSLVPN安全网关建立TLS连接，且使用的国外密码算法套件安全强度足够，此时网络和通信安全层面的“通信数据完整性”、“通信过程中重要数据的机密性”指标该如何进行量化和风险判定？	新增			
13		19.合规密码产品的设备层身份鉴别、完整性相关指标的判定	问题：合规密码产品网络和通信安全层面的“网络边界访问控制信息完整性”指标，以及设备和计算安全层面的“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？	补充合规密码产品网络和通信安全层面的“网络边界访问控制信息完整性”指标的判定说明	18.合规密码产品的设备层身份鉴别、完整性相关指标的判定	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？	
14	20.应用和数据安全层面的测评对象识别与确定	20.4 问题：信息系统的关键数据，通常以生产数据（存储在生产环境中）和备份数据（存储在备份环境或备份介质中）的形式呈现。信息系统使用了第三方提供的数据异	细化备份数据测评规则。补充合并处理时需按两个对象测	19.应用和数据安全层面的测评对象识别与确定	19.4 问题：信息系统的关键数据，通常以生产数据（存储在生产环境中）和备份数据（存储在备份环境或备份介质中）的形式呈现。信息系统使用了第三方提供的数据异地备份的服务，如备份		

			地备份的服务，例如备份在第三方提供的异地机房中，此类备份数据是否纳入测评范围？	评，数据有差别则分别测评。		在第三方提供的异地机房中，备份数据是否纳入测评范围？	
15		22.重要数据机密性、完整性保护的实现方法问题	22.3 问题：鉴别数据使用SM3加盐（salt）杂凑实现重要数据存储机密性如何进行判定。	新增	21.重要数据机密性、完整性保护的实现方法问题		
16		23.应用和数据安全层面的存储机密性问题	问题：在实现数据的存储机密性保护时，未对数据内容（信源）进行加密，而是使用数据整体加密，达到加解密过程对应用软件“无感”的效果。对这种情况进行测评时，应重点关注哪些内容。	新增			
17					22.如何编写涉及应用和数据安全层面的测评内容报告	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？	删除
18					27.如何开展信息系统密码应用成熟度极低情况下的密码应用管理测评	问题：针对部分存量信息系统自身密码应用成熟度极低，未部署任何密码产品对其业务进行密码安全防护，而导致密码应用管理方面无法配套建设的情形，在测评时该如何把握？	调整题目顺序
19	三、密码应用管理类	28.定期开展密码应用安全性评估及攻防对抗演习指标的合规性判定	问题：被测信息系统为试运行阶段开展密评的新建系统，建设运行层面“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”测评项应如何判定？	新增			
20		29.应急处置指标的合规性判定	问题：在部分信息系统从未发生任何密码安全事件的情况下，“事件发生后，应及时向信息系统主管部门进行报告”和“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”指标该如何判定？是否可以判定为不适用？	新增			
21	四、整体测评类	30.测评对象间的弥补场景	问题：测评对象间弥补的场景有哪些？在什么情况下，测评对象A可以弥补测评对象B的分值？	新增			

22	五、 量化 评估 类	31.《商用密码应用安全性评估量化评估规则（2023版）》中，密码使用有效性D项的判定	问题：被测信息系统在实现其密码应用安全需求时，如果使用了存在安全问题或安全强度不足的密码算法，密码算法/协议合规性如何进行量化评估？	安全强度≥112比特的密码算法举例增加HMAC-SHA1	28.《量化评估规则（2023版）》中，密码使用有效性D项的判定	问题：被测信息系统在实现其密码应用安全需求时，如果使用了合规产品中存在安全问题或安全强度不足的密码算法（如DES、MD5等），密码使用有效性D应如何判定和量化？	
23	六、 风险 判定 类	32.有缓解措施的高风险判定	32.1 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？	删除解答“(2)、(3)、(4)”表述	29.有缓解措施的高风险判定	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？	
24			32.2 问题：许多特殊行业的场景（如工控、医疗）不支持直接改造，但依然采用了严格的管理措施来保障风险缓解，高风险判定指引中提到的通用要求和缓解措施无的情况，能否通过严格的管理措施来缓解？	新增			
25					30.报告中对于高风险缓解措施的体现	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？	删除
26		33.应用层身份鉴别是否可以缓解网络层身份鉴别的高风险	问题：“网络和通信安全”“应用和数据安全”的身份鉴别指标有何区别？在测评时如何把握两者的关系？	补充双向风险缓解场景，明确仅能缓解风险不能弥补分值，细化风险缓解逻辑	31.应用层身份鉴别是否可以缓解网络层身份鉴别的高风险	问题：“网络和通信安全”“应用和数据安全”的身份鉴别指标有何区别？在测评时如何把握两者的关系？	
27		35.不涉及高风险的指标使用了高风险算法、技术或产品进行保护时如何判定风险	问题：《信息系统密码应用高风险判定指引（2021版）》不涉及高风险的指标使用了高风险判定指引中列出的高风险算法、技术或产品，例如二级系统的网络和通信层面通信数据完整性，但密码套件的完整性算法出现了高风险算法，应如何判定风险。	新增			
28	七、 特殊 场景 类	37.云平台和云上应用的测评方式和测评结论复用方式	37.3 问题：如果已经取得符合性密评报告的云平台、密码服务平台超期未复评，是否可以被云上应用复用？	新增			
29		39.特殊网络系统的测评对象选取	问题：针对这种纯网络系统，如何开展密评工作？网络和通信安全、设备和计算安全、应用和数据安全层面的测评对象如何选取？	细化纯网络系统测评规则。明确应用和数据安全层面需考	36.特殊网络系统的测评对象选取	问题：针对这种纯网络系统，如何开展密评工作？网络和通信安全、设备和计算安全、应用和数据安全层面的测评对象如何选取？	

				考虑网络管理相关应用及重要数据；用户面通道可不列为测评对象。			
30		41.特定行业或具有特殊密码应用需求的信息系统测评	问题：特定行业的密码应用标准规范与GB/T39786-2021不一致时（存在特殊指标时）应如何确定测评指标、进行量化评估与风险判定？	新增			

# 一、通用类

## 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 22239-2019《信息安全技术 网络安全等级保护基本要求》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。

### 1.1 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 39786-2021 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 39786-2021 第二级密码应用基本要求，以此类推。

### 1.2 问题：

如果新建信息系统在规划阶段尚未完成网络安全等级保护备案工作，被测单位只有一个拟定的信息系统等级，针对此情况如何确定被测信息系

统的密码应用等级？

**解答：**

对于未完成网络安全等级保护定级的重要信息系统，优先以被测单位拟定等级开展密评，但应尽量保证拟定等级与后期备案等级的一致性；如果拟定等级低于后期备案等级时，需要按备案等级重新开展密评。对于无拟定等级的重要信息系统，其密码应用等级至少为第三级。需要说明的是，GB/T 39786-2021 只是密码应用基本要求，被测系统有高安全保护需求或高安全标准等特殊情况，信息系统的密码应用等级可以高于等保定级。

**1.3 问题：**

目前，部分系统责任单位由于上级单位或者政策的要求，希望能够尽可能以高安全标准要求来进行信息系统的安全防护，特别是老旧系统。针对网络安全保护等级为二级的信息系统，被测单位希望能以 GB/T 39786-2021 中的第三级密码应用要求进行改造和测评，此时该如何把握？

**解答：**

目前，GB/T 39786-2021 中的密码应用等级一般与网络安全等级保护的级别持平。所以，在信息系统不存在额外密码应用需求的前提下，原则上被测系统密码应用等级的选取与网络安全等级保护的级别保持一致。但是，针对被测单位以高安全标准规划、建设信息系统的密码应用，并希望能够按照 GB/T 39786-2021 中更高密码应用等级进行密评的情形，密评机构在测评前，应在确认该做法符合被测信息系统所属密码管理部门相关要求的前提下，加以确认其密码应用等级是否等于或者高于等级保护备案等级，进而开展测评工作。

## 2.具有认证证书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。2025 年 4 月 30 日，国家密码管理局发布《关于调整商用密码检测认证业务实施的公告》，2025 年 6 月 30 日前，持证单位可对有效期内《商用密码产品认证证书》申请更换为商用密码检测认证中心颁发的《商用密码产品认证证书》。

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 2020 年换证的密码产品，如果其换发的认证证书上没有标注密码模块安全等级，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，按“密码产品符合一级密码模块”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种类，其他种类产品（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，2025 年 7 月 1 日之后采购的商用密码产品，其认证证书颁发单位应为“商用密码检测认证中心”，如果仍持商用密码检测中心颁发的认证证书，则可能为过期失效的证书，其产品应判定为不合规。

### 3.经认证合格的密码产品的产品合规性、密钥安全符合性的判定要点

## 背景：

GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》的通用测评要求中，提出了对密码产品、密码服务和密钥管理测评要求，相关内容在技术测评要求中进行了引用。

### 3.1 问题：

在密评时，会发现商用密码产品认证证书过期的情况，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，针对这种情况该如何判定密码产品的合规性？

### 解答：

如无特殊情况和安全风险，密码产品的采购合同签订时间如果在商用密码产品认证证书的有效期内，则可判定为产品合规。此外，在测评过程中，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。

### 3.2 问题：

有些类型的密码产品部署模式为客户端与服务端共同作用，实现密码技术的应用。例如，VPN 等密码产品存在客户端和服务端的情况，在测评时应如何判断实际部署中涉及客户端的密码产品的合规性？

### 解答：

可分以下三步依次执行测评实施，综合判定产品的合规性。

一是确认商用密码产品认证证书中的内容是否包括客户端和服务端。通过查看认证证书确定密码产品中是否包括客户端和服务端，还是仅为其一。若无法根据认证证书直接确定，则还需要厂商配合提供密码产品的认证证书对应的检测报告，以进一步确定。

二是确认被测系统中部署的密码产品与送检产品密码边界的一致性（注：这一步主要考虑的情形是认证证书中标明了密码产品包含客户端和服务端。若客户端和服务端本身为两个独立的经检测认证合规的密码产品，则直接分别判定产品合规性即可，此处不再赘述）。根据认证证书和认证证书对应的检测报告，除了确认服务端的一致性之外，如果密码产品包含客户端且对客户端有安全要求，也需要核查客户端与实际产品的一致性。原则上应确保实际部署的密码产品与送检产品的密码边界是一致的，且部署产品版本与送检产品版本一致。如果不一致，则可考虑根据实际密码应用需求及密码使用情况等因素，对产品合规性进行分析判定。例如，送检产品包含安全浏览器和 SSL VPN 网关，实际部署时改为通用浏览器和 SSL VPN 网关，则根据实际密码应用需求进行判定，如仅需实现对服务端的单向鉴别，则测评时重点核查服务端的密码产品合规性，同时核查浏览器是否配套实现了对应的 SSL 协议套件。

三是确认被测系统中部署的密码产品实现的密码功能与送检产品密码功能的一致性。需结合认证证书对应的检测报告，确认被测系统密码应用方案中所描述的拟使用的产品密码功能或被测系统实际使用时所调用的产品密码功能，与送检产品所提供的密码功能的一致性。

### 3.3 问题：

如何确定密码产品的密码功能边界，例如，签名验签服务器实现了加解密功能，在测评时如何判定其合规性？

### 解答：

签名验签服务器是为应用实体提高数字签名、签名验签等运算功能的服务器。签名验签服务器在产品检测时，依据 GM/T 0029《签名验签服务器技术规范》和 GM/T 0028《密码模块安全技术要求》进行检测。在检测过程中签名验签服务器送检厂商会选择支持三类接口（GM/T 0029 附录 A 定义的接口；GM/T 0029 附录 B 定义的接口和 GM/T 0020 标准定义的接口）中的一类或多类进行检测。其中符合 GM/T 0020 标准接口中包含了加解密接口，测评时需要确认是否实现了 GM/T 0020 的接口，如果实现了，则可以提供加解密功能。因此，只要认证产品的安全等级符合要求且实际

测评时确认了和送检产品密码功能（可提供加解密功能）的一致性，则使用签名验签服务器进行加解密密码应用时可以把签名验签服务器视为合规的密码产品。

### 3.4 问题：

经认证合格的密码产品，GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》中“5.5 密钥管理”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 39786-2021 相应等级的要求，如 GB/T 39786-2021 第三级的信息系统应当采用满足 GB/T 37092-2018《信息安全技术 密码模块安全要求》第二级及以上安全要求的密码产品；

（2）如果被测系统有密码应用方案，应核查系统密钥管理机制是否与方案一致；如果被测系统无密码应用方案或系统密钥管理机制与方案不一致，应分析其密钥体系设计是否合理、实现是否正确；

（3）当密码产品产生的密钥在该密码产品外部进行管理时，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；

（4）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.通过代码实现数据机密性、完整性保护的判定方法

### 背景：

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》在 8.4 节中要求“d)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；e)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；f)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；g)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”。实际测评过程中，发现用户可能使用开源代码的密码运算功能对重要数据实现机密性保护、完整性保护，未使用经认证的商用密码产品。

问题：

未使用密码产品，通过开源或自行开发的代码以软件实现密码运算功能的方式进行数据机密性、完整性保护，测评时应重点关注哪些内容？

解答：

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》和 GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》（涉及量化评估计算时，参考《商用密码应用安全性评估量化评估规则(2023版)》），被测系统采用的密码产品应符合相应等级的密码模块安全要求。对于自研软件实现数据机密性和完整性保护且无法提供任何安全性证明的情况，由于无法判断其密码模块安全等级，而且其采用的密码算法或技术实现安全性以及软实现带来的密钥管理安全性均无法保证，因此判定为“不符合”；对于使用第三方开源密码库实现数据机密性和完整性保护的情况，如果第三方开源密码库是经过长期使用且没有暴露出安全问题的，且正确地使用开源密码库，则可以考虑根据实际核查结果酌情判定为“部分符合”，并给予相应分数。是否存在安全性漏洞，如 OpenSSL 库相关安全问题可查询 <https://openssl-library.org/news/vulnerabilities/>等网站。

## 5.组合密码算法的量化评估和风险判定

背景：

组合使用密码算法实现数据安全保护时，针对该情形的量化评估和风险判定。

**问题：**

有些数据的传输或存储保护，存在组合使用密码技术实现的情形，如使用 DES 算法对数据变换后，再使用 SM4 算法对 DES 加密后的密文进行变换，即 SM4(DES(data))，应如何进行量化评估和风险判定？

**解答：**

由于加密算法的安全强度和算法复杂度、参数规模（密钥长度、分组长度等）等相关，当加密算法组合使用时，只要某一层加密算法安全强度足够，且组合算法不使用同一密钥，那么被保护数据就是安全的（其他弱算法的运算可类似看成“未对明文做安全保护”）。因此，当加密算法组合使用时，量化评估和风险判定结果均依据安全强度较高的算法而定。

另外，由于算法安全强度还和密钥管理、算法实现正确性有关，因此在相应测评对象的风险判定时还需综合 DAK 判定情况进行分析评价。

## 6.如何开展分期规划、改造的信息系统的密码应用安全性评估

**背景：**

在进行信息系统密评时发现，被测信息系统有通过评估的密码应用方案，且方案中明确了该系统是分期做密码改造。例如，由于经费原因，应用和数据安全层面的身份鉴别指标不做改造但给出了合理的风险缓解措施，且明确在二期建设中进行改造并给出改造的密码应用解决方案。在被测系统按照密码应用方案一期建设要求完成建设后，开展密评。

**问题：**

针对上述情况，在信息系统按密码应用方案完成一期建设后开展密评时，该如何确定测评范围？

**解答:**

对于密码应用方案中涉及分期密码改造的情况,在实际测评时,应根据系统定级范围和密码应用需求选取所有适用的测评指标和测评对象开展系统密评并给出评估结论,即测评指标和测评对象的选取范围与该系统是否进行分期密码改造无关。

## 7.已有通过评估的密码应用方案,在实际密评时的注意事项

**背景:**

按照密评管理办法及相关管理要求,网络与信息系统运营者应在系统规划阶段完成密码应用方案评估,在建设和运行阶段完成系统密评。

**问题:**

针对密码应用方案已经通过评估的信息系统,在系统密评时发现实际情况与密码应用方案不一致,如何处理?

**解答:**

密码应用方案评估是在信息系统规划阶段,对所编制的密码应用方案(或密码改造方案)进行评估。建成或已运行的信息系统的密码应用情况是否与规划阶段的一致,需要在系统密评阶段(包括初次密评和定期密评)进行核实、验证,因此在实际开展系统密评工作时,可参考通过评估的密码应用方案等文件了解系统业务和密码应用情况。

如果在测评时发现实际建设情况与密码应用方案不一致,则需要网络与信息系统运营者提供密码应用方案修订或优化的证明材料,但同时应按实际测评时掌握的信息为准,并以实际情况得出测评结果。

## 8.自建 CA 签发数字证书的合规性判定要点

**背景：**

部分企业通过自建 CA，签发数字证书为内部应用提供加密通信、身份认证等安全服务。

**问题：**

企业通过自建 CA 为信息系统签发用于加密通信和身份认证的数字证书，是否合规？

**解答：**

企业可以通过自建 CA 为信息系统签发用于加密通信和身份认证的数字证书，企业签发上述数字证书无需具备《电子认证服务使用密码许可证》或《电子政务电子认证服务机构资质证书》。为保障签发证书的安全性，企业自建 CA 所使用的密码产品应具有商用密码产品认证证书。其使用的密码产品安全等级应与信息系统密码应用要求的等级相符，企业应采取相应的技术和管理措施保障自建 CA 安全运行，特别是数字证书的申请、签发、发布、更新、撤销等全生命周期管理。

**9.对于被测方没有改造和管理权限的接口进行密评的注意事项**

**背景：**

接口对接分为本端提供接口供其他系统连接，以及对端系统提供接口由被测单位去配合连接两种情况，前者被测方有管理权限，有改造权限，后者无改造权限无管理权限，只能被动配合。

**问题：**

是否可以因为无改造和管理权限、接口责任方不在本系统范围等原因将这类互联通道论证为不适用？

**解答：**

虽然在对端系统提供接口，被测单位只能被动配合且无改造和管理权限的情况下，被测单位在该互联通道上的操作和控制能力有限，但这并不

意味着该互联通道就不具有重要性或对系统整体的安全性方面没有影响；不能仅仅因为无改造和管理权限、接口责任方不在本系统范围等原因就将这类互联通道论证为不适用。

确因客观原因无法取得关键证据，可考虑系统实际情况，酌情采用非关键证据对系统指标进行判定。针对被测方没有改造和管理权限接口情况，风险判定时仍需依据《信息系统密码应用高风险判定指引（2021版）》，并结合实际安全控制措施进行判定。

## 二、密码应用技术类

### （一）物理和环境安全

#### 10.物理和环境安全层面的测评对象识别和确定

背景：

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》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，GB/T 43206-2023《信息安全技术 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。

#### 10.1 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及如何开展密评？

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。1) 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开展了商用密码应用安全性评估且相应系统评估结论为“符合”或“基本符合”，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。特别地，如果云平台通过了商用密码应用安全性评估，并且级别不低于云上应用系统的网络安全保护等级时，则云上应用系统的物理和环境安全层面复用云平台相应层面的测评结论。2) 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开展商用密码应用安全性评估或开展了相应系统评估但结论为“不符合”，则密评人员需现场取证；对于条件不允许的情况，可以通过系统建设方或租赁方要求 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。

## 10.2 问题：

当被测信息系统的机房采用多层门禁措施，且不同门禁采取的物理访问身份鉴别机制不一致时，例如外层门禁采用非密码技术，而内层门禁采用经检测认证合格的安全门禁系统实现，则物理和环境安全层面的“身份鉴别”指标该如何选择测评检查点？

## 解答：

针对此情况需要考虑多层电子门禁系统的保护范围。如果信息系统所有的受保护对象都在多层门禁的保护范围之内，则可在多层门禁系统中选择密码应用最合规、正确、有效的进行测评，但要注意多层门禁之间的物理区域存在非授权人员访问情形。如果存在某个受保护对象只在最外层电子门禁系统的保护下，那么应该以最外层的电子门禁系统作为测评对象。

如果受保护对象在多个电子门禁系统的保护下，那么所有提供保护的电子门禁系统都需要测评。几种情况示例如下：

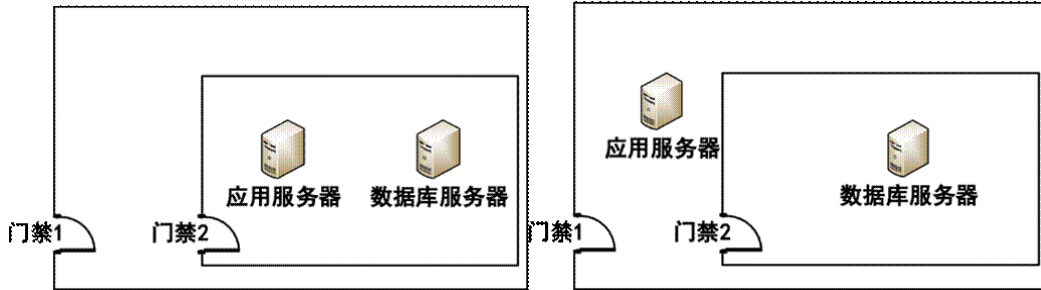


图 10-1 多重保护

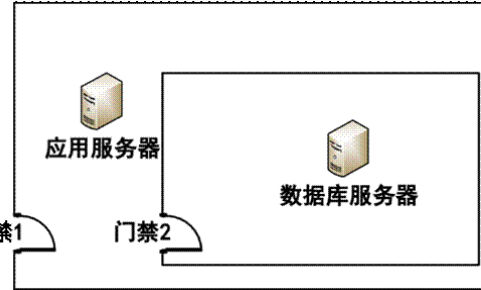


图 10-2 分布在多层门禁中

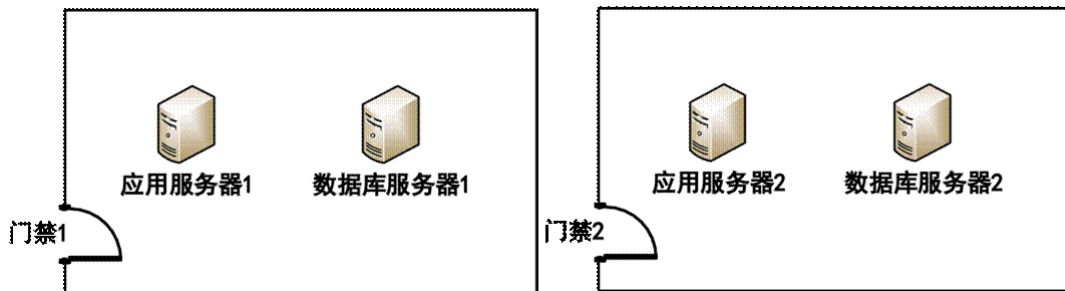


图 10-3 分布在多个门禁中

在上述示例中：

➤图 10-1 中，可选择密码应用最合规、正确、有效的门禁进行测评，测评过程中两个门禁中有一个满足测评要求即可。但是同时要注意，如果门禁 1 与门禁 2 之间物理区域还有非授权人员可以访问的话，则必须对门禁 2 测评；而外层门禁可能会起到安全加固和安全风险缓解作用，密评机构需根据实际情况进行确认。

➤图 10-2 中，应选择门禁 1 测评。

➤图 10-3 中，门禁 1 和门禁 2 需要作为两个测评对象进行测评。

## 11.电子门禁记录数据存储完整性测评时的注意事项

背景：

一些信息系统所在机房已经部署合规的电子门禁系统，厂商也声称机房进出记录受到完整性保护。

问题：

对于符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》标准的电子门禁系统，其门禁系统内置的进出记录数据存储的完整性保护是否可以直接采信产品检测结果，如不可直接采信，是否需要门禁系统厂商提供其他证据？

**解答：**

由于 GM/T 0036-2014 中规定的相关要求，主要针对的是采用基于非接触式卡的门禁系统对机房进出人员身份鉴别这一场景，因此，对门禁系统进行密评实施时，按照密评相关标准，需要相关密码厂商提供门禁系统进出记录数据存储完整性保护的相关证据，并提供实现该密码应用的密码产品检测认证合规性的证明。

## **（二）网络和通信安全**

### **12.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 39786-2021《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。

#### **12.1 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路区域访问被测系统。

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,使用支持商用密码的浏览器(以下简称“国密浏览器”)或不支持商用密码的浏览器(以下简称“非国密浏览器”)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。

### 12.2 问题:

当被测系统使用第三方电子认证服务机构提供的认证服务完成系统功能时,被测系统与第三方电子认证服务相关系统之间的通信信道是否需要纳入测评范围?

### 解答:

如果被测系统与第三方电子认证服务相关系统之间的通信信道经过了不可控的网络环境(比如互联网等),该条通信信道应该纳入“网络和通信安全”层面的测评对象进行测评。同时要注意到,CA 相关标准已经规定了 CA 系统与 OCSP/CRL/RA 服务器之间的应用层安全通信协议;对于普通用户证书查询,可能不涉及重要数据的机密性保护,数据来源完整性已通过 CA 等服务端的签名做了防护;另外,若应用系统使用 GM/T 0148 《证书认证注册子系统证书服务接口规范》与 CA 系统进行通信,需要遵循 GM/T 0148 的要求将该安全通信信道纳入“网络和通信安全”层面的测评对象进行测评。

### 12.3 问题:

若被测系统为独立的内网系统,且不允许跨网络边界进行远程运维,这种情况下在网络和通信安全层面是否可认为没有测评对象?

### 解答:

这类情况下还需要确定网络边界环境及网络内部的安全性,再行决定。

网络和通信安全层面的测评对象的选择,不仅仅以系统属于的网络环境是内网还是外网进行区分,应以系统所在的网络边界环境,以及网络内部通信是否安全作为网络和通信层面是否需要测评的标准。

#### 12.4 问题:

针对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无论是通过运营商专线还是采用物理裸光纤进行数据通信,均应将该通信信道作为测评对象并参照 GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》进行测评。

双活机房之间的通信链路采用运营商专线:由于运营商专线中间经过运营商的各类路由交换设备,存在非授权访问篡改的安全风险,该通信链路应作为网络和通信安全测评的重点对象。

双活机房之间的通信链路采用裸光纤:主要分为两种情况。

(1) 短距离链路:对于物理上处于同一建筑物或相邻楼宇之间的通信链路,通常情况下其面临的安全威胁相对较小,若具备足够的物理安全防护(如专用机房、链路隔离、监控设施等),或机房间不涉及不可控交换设备(一般这种情况都不涉及到不可控交换设备),且没有跨越网络边界或外部开放的潜在风险,可不作为独立的测评对象。需要注意的是,即使为短距离链路,也应在密码应用方案中明确链路的实际安全控制措施,并经密评机构审定后按实际情况处理。

(2) 跨区域、长距离链路:对于跨越较长物理距离的同城、异地机房的通信裸光纤链路,裸光纤不涉及中间的不可控交换设备,可不作为独立的测评对象。但因其涉及外部传输和更复杂的安全控制要求,若不将该通信信道作为网络和通信安全层面的测评对象,则应在密码应用方案中详细说明该通信链路的实际情况并经密评机构审定后按实际情况处理。其中,通信链路的实际情况包括但不限于自建或租用情况、传输数据的方式、传

输数据的内容、链路的物理位置和节点受控情况等。

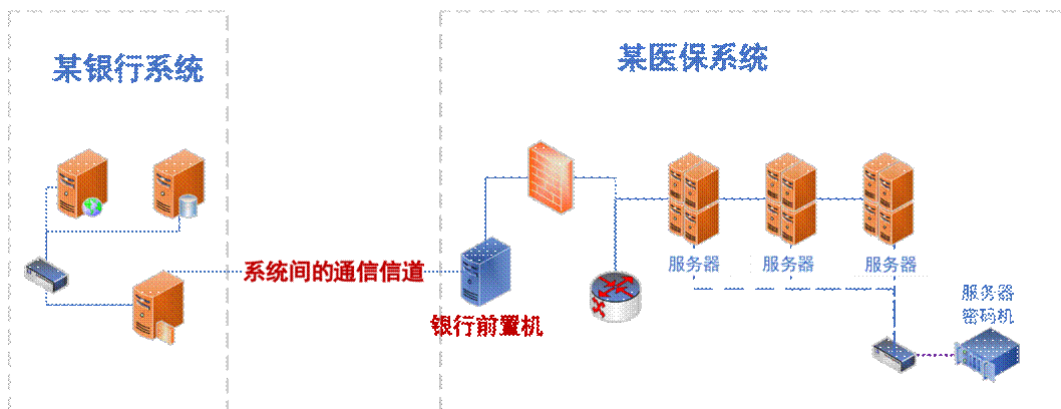
## 12.5 问题：

跨网络边界的系统之间的交互，如果通信主体不在其责任范围之内，例如，被测系统与外部系统通过前置机建立通信信道，前置机部署在被测系统内且不属于被测系统责任单位，此通信信道是否需要纳入测评范围？比如医保系统与银行系统有业务往来，医保系统外联出口处放置银行前置机，作为与银行系统交互的中间设备，银行前置机与银行系统之间搭建了通信信道。

## 解答：

跨网络边界的系统之间的交互所搭建的通信信道，无论通信主体是否属于被测系统，该通信信道都应纳入“网络和通信安全”层面的测评对象进行测评。

比如医保系统与银行系统有业务往来，医保系统前放置银行前置机，由银行前置机跟医保系统交互，再由银行前置机与银行系统搭建通信信道。如图 12-1 所示：



**图 12-1 存在系统间通信信道的场景**

该图中，银行前置机归属于银行系统责任单位，则在测评医保系统时，在“网络和通信安全”层面也需要测评“系统间的通信信道”（图中所示）。

## 12.6 问题：

如果服务端同时支持国外和国密算法，如何选择该通道的测评对象？

**解答：**

若客户端未采用技术手段限制算法类型，也就是同一个用户可以选择核准的算法套件也可以选择非核准的算法套件，则现场测评时依据就低原则进行测评，即选择该通道最不符合测评条款的算法类型进行测试和量化评估，按照该通道最弱的算法套件计分；若客户端和服务端采用了技术措施限制算法使用的类型，但仍存在用户客户端支持国密浏览器建立国密通道，同时也支持非国密浏览器建立非国密通道，两类情况同时存在日常不同用户的使用中，比如用户群体 A 使用国密套件，而用户群体 B 使用非国密套件，则两类通道需作为两个对象进行测评。

### 13.网络和通信安全层面的身份鉴别等指标

**背景：**

SSL VPN 安全网关除了支持符合国家或密码行业标准要求的安全传输服务以外，往往也支持基于国外密码算法的安全传输服务。很多应用系统往往会使用通用浏览器和 SSL VPN 安全网关相搭配的安全传输服务。

#### 13.1 问题：

采用合规的 SSL VPN 安全网关建立 TLCP 连接，但客户端采用的浏览器（插件）或客户端软件未获得商用密码产品认证证书，此时网络和通信安全层面的“身份鉴别”指标该如何进行判定？

**解答：**

如果客户端的浏览器与服务端建立 TLCP 连接，且是客户端对服务端的单向身份鉴别，由于考虑到客户端没有私钥管理需求，如果采用了国密算法套件，在能够保证签名验证算法实现正确、服务端数字证书验证有效情况下，按照《商用密码应用安全性评估量化评估规则（2023 版）》，最高可判定为“D(√)、A(√)、K(√)。”但是必须充分认识到，此时的客户端软件在随机数产生、密码算法实现自测试方面仍有一定的风险，鼓励密码

厂商将提供 TLCP 单向认证功能的客户端软件提交商用密码产品检测认证。

针对网络和通信安全层面的“双向身份鉴别”，由于在客户端需要进行私钥管理，如果采用的是不具备商用密码产品认证证书（或密码模块等级不符合）的浏览器或客户端软件，则密钥管理 K 应判为“不符合”，且按照《信息系统密码应用高风险判定指引（2021 版）》相关条款开展高风险判定。

### 13.2 问题：

当用户使用“合规”的 SSL VPN 安全网关建立 TLS 连接，且使用的国外密码算法套件安全强度足够，此时网络和通信安全层面的“通信数据完整性”、“通信过程中重要数据的机密性”指标该如何进行量化和风险判定？

### 解答：

首先需要明确，具有商用密码产品认证证书的 SSL VPN 安全网关，在产品检测和认证时并不对其向业务用户提供的 TLS 连接功能进行检测，因此该功能并没有被检测认证过。所以，在对该功能进行密评时不能复用 SSL VPN 产品检测认证的结果。量化评估时，D、A、K 最高可判定为“D（√）、A（×）、K（×）”，同时按照《信息系统密码应用高风险判定指引（2021 版）》相关条款开展高风险判定。

## 14.网络层安全接入认证和身份鉴别指标的差别

### 背景：

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》在 8.2 节中要求 e)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，确保接入的设备身份真实性。

### 问题：

如何理解“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,确保接入的设备身份真实性”?安全接入认证和身份鉴别如何进行区分?

**解答:**

“身份鉴别”指标适用于两个实体通过不可控的网络(比如互联网)进行通信之前进行的身份鉴别,比如IPSec VPN或者SSL客户端/服务器的场景,IPSec VPN之间或者SSL客户端和服务端之间的鉴别都属于“身份鉴别”指标的测评范围。

“安全接入认证”指标适用于设备“物理地”从外部接入信息系统的内部网络之前对设备的身份鉴别,接入后,该设备将成为信息系统内部网络的一部分。比如智能手持移动终端设备接入信息系统网络的场景,对于移动智能终端设备接入的认证属于“安全接入认证”指标的测评范围,该类终端设备经认证接入信息系统网络后则成为网络内的一部分。

### **(三) 设备和计算安全**

#### **15.设备和计算安全层面的测评对象识别与确定**

**背景:**

GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》在设备和计算安全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:**

设备和计算安全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，对设备和计算安全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、虚拟设备和系统。

## 16.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。

## 17.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。

### 17.1 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(2021版)》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。

## 17.2 问题:

设备和计算安全层面,如果信息系统通过堡垒机统一运维管理设备,堡垒机及其被运维设备的身份鉴别指标如何进行判定?

## 解答:

在合规性判定方面,各设备的身份鉴别应分开判定,例如,堡垒机采用动态令牌系统登录,使用用户名+口令登录应用服务器等被运维的设备,则堡垒机的身份鉴别可判定为“符合”,但被运维设备的身份鉴别应判定为“不符合”。

在风险判定方面,遇有以下情况可以酌情降低风等级:

(1)直接通过堡垒机运维,如果堡垒机的身份鉴别没有高风险,则通过堡垒机进行统一管理的设备,其身份鉴别可视为采取了风险缓解措施;

(2)通过 VPN 保护运维通信信道,同时满足以下条件则堡垒机及其被运维的设备,其身份鉴别可视为采取了风险缓解措施:

a.VPN 是运维专用的安全网关,运维人员也无法绕过安全网关进行设备远程运维管理(如堡垒机仅对 VPN 地址开放远程管理端口并限制堡垒机从本地登录);

b.VPN 客户端与安全网关之间的通信信道采用密码技术进行通信实体双向身份鉴别,并且在客户端鉴别时须使用运维人员所持智能密码钥匙等存有身份鉴别信息的硬件介质进行实现(需注意每次设备运维时须重新建立 VPN 连接);或者,运维人员登录 VPN 设备进入内网时采用动态

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且机制正确、有效。

## 18.远程管理通道安全的测评要点

### 背景：

GB/T 43206-2023《信息安全技术 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安全、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安全、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的，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。

## 19.合规密码产品的设备层身份鉴别、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：

合规密码产品网络和通信安全层面的“网络边界访问控制信息完整性”指标，以及设备和计算安全层面的“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,并且部署产品的密码模块等级符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中规定的对各级信息系统的安全等级要求的情况下,考虑到安全等级二级及以上的密码产品自身安全防护能力较高且采用基于核准的数字签名或带密钥消息鉴别码技术实现软件/固件的完整性校验,针对整机类密码产品在设备和计算安全层面的“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”这三个指标,可判定为“符合”。对于安全等级一级的整机类密码产品,量化评估的 D、A、K 可判定为“√√×”,并考虑产品等级的修正 Rk。

网络和通信安全层面采用了合规网络密码产品,如 IPSec/SSL VPN 网关的“网络边界访问控制信息完整性”指标判定,可以此类推。

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)、是否按照密码产品使用要求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。特别地,如果配套的终端类密码产品(如智能密码钥匙、智能 IC 卡等)没有独立的商用密码产品认证证书,或者不包含在该整机类密码产品的商用密码产品认证证书对应的检测报告中,则可判定“身份鉴别”指标的“密钥管理安全性”为“不符合”。

对于没有“商用密码产品认证证书”而仅具有“密码检测证书”的密码产品,如某些行业采用了经国家密码管理部门认可的专用算法研制的产品,其虽然没有认证证书但具有检测证书,同样依据相关标准通过了检测,是经过国家密码管理部门认可的,应该将其判定为合规产品。另外,针对此种情况,还需核查产品实际使用范围与检测证书上所标注范围的一致性。

#### **(四) 应用和数据安全**

##### **20.应用和数据安全层面的测评对象识别与确定**

## 背景：

GB/T 43206-2023《信息安全技术 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”。

### 20.1 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，具体参考已通过评估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。

### 20.2 问题：

在云应用/平台测评中，密码资源池的密码管理平台应作为应用和数据安全层面的测评对象，还是设备和计算安全层面的测评对象？

### 解答：

通常在云平台建设过程中，会搭建密码资源池，统一为云上应用提供密码计算、密码服务等资源，密码管理平台是对若干台密码设备的统一调度管理平台，在对云平台密码资源池里的密码设备进行运维管理的同时，建立统一的密码服务接口，面向云平台上的所有应用系统提供密码接口服务，业务逻辑复杂，是云上系统实现密码应用的重要支撑，故应将其作为应用和数据安全层面一个管理类应用系统进行测评。

### 20.3 问题：

信息系统通过前端设备采集数据，并且在前端会有存储设备或功能模块收集相关数据，这部分数据是否需要纳入测评范围？

### 解答：

应结合信息系统所在行业关于数据分级的标准和要求，以及信息系统的网络安全等级保护测评报告和密码应用方案（或密码改造方案）进行相关数据重要程度的确定。将所确定的重要数据纳入测评范围，并根据数据实际安全需求开展测评。

#### 20.4 问题：

信息系统的关键数据，通常以生产数据（存储在生产环境中）和备份数据（存储在备份环境或备份介质中）的形式呈现。信息系统使用了第三方提供的数据异地备份的服务，例如备份在第三方提供的异地机房中，此类备份数据是否纳入测评范围？

#### 解答：

备份数据作为生产数据的副本，其数据属性和安全等级不因存储位置变化而发生改变，其密码应用需求原则上应与生产数据一致。在测评时，应分别核查原始生产数据和备份数据的密码应用需求是否得到满足。特别地，若采用第三方提供的数据异地备份服务，由于涉及系统间通信，还应注意核查数据备份时跨网络传输的安全性。

在编写密评报告时，通常可考虑将备份数据同生产数据合并处理，作为同一个业务类重要数据体现。若存在备份数据的密码应用需求没得到满足情况，应体现在该项重要数据的相应测评项结果判定中。例如，合并对象后的生产数据的存储机密性为“符合”，备份数据的存储机密性为“不符合”，则该项重要数据的存储机密性，按照两个对象测评，结果为“部分符合”，其完整性，如果确保两端数据完全一致，可考虑将两个对象采用了其中一个（比较好的）完整性保护措施保护；数据有差别，例如非实时更新，则应作为两个测评对象分别测评。

## 21.应用和数据安全层面的身份鉴别

### 背景：

大量应用系统的身份鉴别使用第三方提供的身份认证服务（此处特指第三方身份认证服务为已单独等保定级的系统）。例如，采用政务集约化建设模式，应

用系统用户由第三方（包括统一身份认证平台等）提供的身份认证服务进行身份鉴别。此外，某些应用系统在与其它系统对接时也存在身份鉴别的需求。

**问题：**

对于此类提供身份认证服务的第三方系统是否要求通过密评后再提供身份认证服务？若该第三方系统未通过密评，是否可以直接认为其应用和数据安全层面的“身份鉴别”指标为“不符合”？

**解答：**

对于已通过密评（“符合”或“基本符合”）的第三方身份认证服务系统，应用和数据安全层面“身份鉴别”指标经过了完整的密码测评，对业务应用系统进行该指标核查时，在确认第三方身份认证服务的有效性后，可复用该指标相关结论；此外，由于调用第三方身份认证服务涉及到系统间通信，所以还需对在鉴别机制工作过程中涉及到的重要数据的传输安全性进行延伸测评。

对于未通过密评或未做密评的第三方身份认证服务系统，在测评业务应用系统时，测评人员应对第三方系统所提供的身份鉴别机制及其鉴别机制工作过程中涉及到的重要数据的传输安全性进行延伸测评。再进一步，如果第三方身份认证系统上保存有应用系统的身份鉴别信息，应对第三方身份认证服务系统上相关的密码应用进行（重新）测评，例如，重要数据存储的机密性和完整性。对于测评条件不允许的情况，可以要求第三方身份认证服务的系统责任方提供相关说明文件和证据以支撑测评结论。

在上述情况中，如果存在跨网络区域调用的情况，还需要考虑被测系统与第三方身份认证服务系统之间的“网络和通信安全层面”的测评。

## 22.重要数据机密性、完整性保护的实现方法问题

**背景：**

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的应用和数据安全层面涉及到重要数据的机密性和完整性保护要求。在实际测评时，可能遇

到一些算法选用方面的问题。

### 22.1 问题：

对于数据库中的重要数据存储完整性保护，仅使用 SM3 进行保护能否判定为“符合”？

### 解答：

仅使用 SM3 算法实现数据存储完整性功能，在安全机制方面存在缺陷。入侵者可在篡改数据后，重新进行 SM3 杂凑运算并覆盖原先的杂凑值。因此，应判定为“不符合”。

因此建议使用合规的密码产品通过 HMAC-SM3、基于 SM4 的 MAC（参考 GB/T 15852.1-2020《信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制》）或数字签名的方式实现数据存储的完整性。

### 22.2 问题：

使用经检测认证合格的服务器密码机（符合相应等级的密码模块安全要求）中的 SM4-ECB 算法（密钥管理由服务器密码机完成）对重要数据进行机密性保护，能否判定为“符合”？

### 解答：

分组密码的 ECB（电码本工作）模式，因其特殊的工作流程，无法隐蔽数据模式（如使用同一个密钥会导致相同的明文分组产生相同的密文分组），也不能抵抗对分组的重放、嵌入、删除等攻击。因此，对于超过一个分组长度的明文一般建议不使用 ECB 工作模式，并根据《信息系统密码应用高风险判定指引（2021 版）》给出风险判定。对于可接受重复性（例如，输入分组绝不重复），必须单独访问或随机访问各个分组的特殊使用情况，按照现行准则，可以酌情考虑允许使用 ECB 模式，并进一步核实是否采取了必要的风险缓解措施，给出符合性判定和风险判定。

### 22.3 问题：

鉴别数据使用 SM3 加盐（salt）杂凑实现口令存储机密性保护，如何进行判定。

**解答：**

采用加盐杂凑的方法对口令进行不可逆计算是对口令的常见保护方法，可以有效防止字典攻击。在保证盐值唯一（每个用户盐值不同）、口令强度和登录次数限制的情况下，能够一定程度上满足口令本身的机密性保护要求。推荐采用国家密码管理部门核准的密码模块实现 SM3 杂凑算法，同时保证盐的长度和算法迭代轮数满足 GM/T 0091-2020《基于口令的密钥派生规范》的要求。

另外，上述方法仅能用于口令本身的机密性保护，为防止口令被整体或部分篡改、替换等，还需要加入对口令的完整性，以及访问控制等保护措施。

### 23.应用和数据安全层面的存储机密性问题

**背景：**

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的应用和数据安全层面涉及到重要数据的机密性保护要求。在实际测评时，存储加密可能遇到不同的加密方式。

**问题：**

在实现服务端数据的存储机密性保护时，未对数据内容（信源）进行加密，而是使用加解密模块等产品对数据整体加密，达到加解密过程对应用软件“无感”的效果。对这种情况进行测评时，应重点关注哪些内容。

**解答：**

服务端对重要数据加密或完整性保护可能实施在不同层次上，包括物理层（如磁盘加密）、设备层（操作系统或数据库直接加密）、应用层（文件/数据库表加密）以及以上多层方式的组合等。对于不同层次的加密措施，其防护的对象和面临的风险也不同，因此需要根据实际情况综合判断。

根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中应用和数据安全层面的要求，重要数据的存储机密性和传输机密性，均

为对数据资源本身提出的密码应用要求，因此，对于该项指标实现的符合性判定，应以应用对数据资源本身是否进行加密为准。

在应用和数据安全层面，判定重要数据资源的传输机密性时，以数据资源（信源）是否加密为准，同理，判定重要数据资源的存储机密性时，也应以应用是否对数据资源本身加密为准。

数据加密的形式可分为以下三种情况：

（1）对于数据整体的物理层加密存储，仅能防止设备或存储介质被窃取或复制时可能导致的数据泄露风险。此时，需要根据信息系统实际安全需求，确定上述技术手段是否能够有效应对信息系统面临的数据安全威胁。

（2）如果数据整体加密实现数据库透明加解密，并且采用了细粒度访问控制，例如基于身份鉴别的访问控制、不同用户数据进行隔离等措施，确认相关措施有效的情况下，可酌情判定密码使用有效性（D）为“√”，并给出风险提示与建议，建议运营者进一步做好对重要数据访问权限的控制。

（3）应用对数据资源本身进行加密，并将加密后的密文数据写入数据库表、文件或对象存储中存储时，在不进行解密的情况下，仅能查看数据密文，这样满足应用和数据层面对数据存储机密性保护的要求，密码使用有效性（D）可判定为“√”。需要注意的是，应用本身一般无法对所有数据都进行加密保护，只对重要数据进行加密保护。

另外，在判断密码使用有效性（D）的同时，还需要关注使用加解密模块等产品的合规性，是否按照安全策略被正确地安装部署、配置和使用，以及所使用的密钥全生命周期管理机制是否合理有效。

## （五）综合

### 24.访问控制信息的具体含义

背景：

GB/T 39786-2021《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、标签等能够决定信息系统应用访问控制的措施等信息。

## 25.跨网络调用密码资源实现相应密码功能的测评要点

### 背景：

信息系统跨网络边界调用密码资源实现其密码应用安全需求时，通常存在两种场景：一是调用主体与密码资源部署在同一机房内，但在不同的网络区域，如部署于互联网区的业务应用系统调用部署于政务外网区的密码资源；二是密码资源与调用主体部署于不同机房，如某地建立统一密码服务平台为各类信息系统提供密码应用支撑，统一密码服务平台与信息系统并非在同一个机房中部署，信息系统机房与统一密码服务平台机房之间建立安全通信信道进行数据传输。

### 问题：

针对于跨网络边界调用密码资源的情况，在测评时应重点关注哪些问题？

### 解答：

跨网络边界调用密码资源打破了传统密码设备本地调用的安全假设，非必要情况不建议跨网络边界调用密码资源。

GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》在网络和通信安全层面的测评对象为“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”。被测信息系统跨网络边界调用密码资源(如服务器密码机、统一密码服务平台等)时，该调用通道应作为网络和通信安全层面的测评对象进行“身份鉴别”“通信数据完整性”“通信过程中重要数据的机密性”“网络边界访问控制信息的完整性”等指标的测评，同时应结合系统现状综合分析远程调用密码资源带来的数据泄露等安全风险。

另外，在涉及密码资源调用的技术指标测评时，针对密钥管理安全（K），除关注密码产品/密码服务的合规性、密钥生命周期管理机制的安全性外，还应关注具体密码资源调用时的鉴别与访问控制机制，即核实密码资源（如密码服务平台）和具体密码功能是否被授权的合法实体访问和调用。

### 三、密码应用管理类

#### 26.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 9.7a)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 GB/T 43206-2023《信息安全技术 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 GB/T 43206-2023 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（2021版）》进行风险评价。

#### 27.投入运行前未进行密码应用安全性评估的合规性判定

背景：

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》8.7 节 d)条款规定“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”，但很多已建信息系统并没有在投入运行前进行密码应用安全性评估。

问题：

被测信息系统为已建运行系统，其建设完成时未进行投入运行前的商用密码应用安全性评估；或者，被测信息系统经密码应用改造后，在重新

上线前进行了商用密码应用安全性评估。建设运行层面“投入运行前进行密码应用安全性评估”测评项应如何判定？

**解答：**

“投入运行前进行密码应用安全性评估”测评指标的合规性判定以密码法实施时间为界限。

(1) 2020年1月1日之前投入运行的信息系统：密评时该项可判定为“不适用”；

(2) 2020年1月1日之后投入运行的信息系统：如果其建设完成后未进行投入运行前的密码应用安全性评估，则密评时该项判定为“不符合”。

以上情况中，若被测信息系统后期依据通过评估的密码应用方案进行了密码应用改造，在重新投入运行前进行了密码应用安全性评估且评估结论为“符合”或“基本符合”（注：系统通过密评的条件仅针对遵照 GB/T 39786-2021 中密码应用第三级和第四级的信息系统，第一级和第二级的信息系统只要求开展密评），此时投入运行时间可按照密码应用改造后重新上线的时间进行确定，该项可判定为“符合”。

需要说明的是，对于分期进行密码保障系统建设的情况，投入运行时间原则上按照第一期建设完成后的上线时间进行确定。对于分期密码建设的第三/四级信息系统，可酌情结合系统建设实际情况，将投入运行时间点后延（如确因经费等客观因素所限，导致第一期建设的密码应用成熟度尚存在差距，可考虑投入运行时间按后期改造完成的上线时间进行确定），判定方法如上所述。

## 28.定期开展密码应用安全性评估及攻防对抗演习指标的合规性判定

**背景：**

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》8.7节 e)条款规定“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”，但很多信息系统是处于试运行阶段的新建系统，并在试运行阶段开展密评工作。

**问题：**

被测信息系统为试运行阶段开展密评的新建系统，建设运行层面“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”测评项应如何判定？

**解答：**

根据 GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》7.3.5.3 测评实施中“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”的要求，若被测系统处于试运行阶段开展密评工作，则仅需查看相关的管理制度中是否有对信息系统投入运行后定期开展密码应用安全性评估及攻防对抗演习的要求，若管理制度中提及相应的要求，则可判定为“符合”。同时应关注后续正式运行过程中的实际情况，查看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，根据评估结果制定整改方案，并进行整改。

## 29.应急处置指标的合规性判定

**背景：**

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》8.8 节 b)条款规定“事件发生后，应及时向信息系统主管部门进行报告”、c)条款规定“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”，但部分信息系统从未发生任何密码安全事件。

**问题：**

在部分信息系统从未发生任何密码安全事件的情况下，“事件发生后，应及时向信息系统主管部门进行报告”和“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”  
指标该如何判定？是否可以判定为不适用？

**解答：**

在未发生任何密码安全事件的情况下，指标仍判定为“适用”，无论是否有安全事件发生，均应具有相应的体系、制度、执行表单等文档材料。虽然密码安全事件尚未发生，但被测单位仍需具备相应应急制度，同时需要查看是否有对应的执行记录模版。

## 四、整体测评类

### 30.测评对象间的弥补场景

**背景：**

根据 GM/T 0116-2021 《信息系统密码应用测评过程指南》，在完成单元测评后，需针对测评结果为“部分符合”和“不符合”的测评对象，采取逐条判定的方法，给出整体测评的具体结果；经过整体测评后，有的测评对象的测评结果可能会有所变化，需要进一步修订测评结果。《商用密码应用安全性评估量化评估规则（2023 版）》给出了测评对象分值修订的原则，即：若测评对象 A 弥补了测评对象 B 的不足，测评对象 A 的分值为  $P_A$ ，测评对象 B 的弥补前分值为  $P_B$ ，则测评对象 B 弥补后的分值为  $\text{MAX}(0.5 \times P_A, P_B)$ ，即  $0.5 \times P_A$  和  $P_B$  之间的较大值（四舍五入，取小数点后 4 位）。

**问题：**

测评对象间弥补的场景有哪些？在什么情况下，测评对象 A 可以弥补测评对象 B 的分值？

**解答：**

系统密评的整体测评从测评单元间、安全层面间两个方面进行测评和综合分析，即针对测评对象的测评结果为“部分符合”和“不符合”的单个测评项，首先分析与该测评项相关的其他单元的测评对象能否和它发生

关联关系，关联关系产生的作用是否可以“弥补”该测评项的不足；其次分析与该测评项相关的其他层面的测评对象能否和它发生关联关系，关联关系产生的作用是否可以“弥补”该测评项的不足。

目前，可能存在弥补关系的测评项包括“网络和通信安全层面-通信数据完整性”和“应用和数据安全层面-重要数据传输完整性”、“网络和通信安全层面-通信过程中重要数据的机密性”和“应用和数据安全层面-重要数据传输机密性”。例如，网络和通信安全层面存在一条或多条业务通信信道，通过业务通信信道传输应用系统的重要数据，在整体测评时，需要分析“网络和通信安全层面”的业务通信信道与“应用和数据安全层面”的应用系统重要数据是否会发生关联关系，是否能够相互弥补。以应用系统重要数据 A 在“应用和数据安全层面”明文传输为例，需要考虑以下两种情况：

(1) 网络和通信安全层面采用密码技术搭建了相对安全的业务通信信道 B，实现应用系统重要数据 A 在通信过程中的机密性保护，且应用系统重要数据 A 未在其他跨网络边界的通信信道中传输，则测评对象 B 可以弥补测评对象 A 的不足，可参照《商用密码应用安全性评估量化评估规则（2023 版）》对测评对象 A 的分值进行修订。

(2) 应用系统重要数据 A 在多条通信信道中传输，当多条通信信道均采用密码技术实现通信过程中重要数据 A 的机密性保护时，应采取“就低原则”对测评对象 A 的分值进行量化评估；当其中某条通信信道未采用密码技术时，测评对象 A 无法被“网络和通信安全层面”的测评对象弥补。

## 五、量化评估类

### 31. 《商用密码应用安全性评估量化评估规则（2023 版）》中，密码使用有效性 D 项的判定

背景：

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》在 8.4 节中要求“d)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；e)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；f)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；g)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”。实际测评过程中，发现信息系统可能使用合规的密码产品对重要数据实现机密性保护、完整性保护，但使用了如 MD5 的高风险算法。

#### 问题：

被测信息系统在实现其密码应用安全需求时，如果使用了存在安全问题或安全强度不足的密码算法，密码算法/协议合规性如何进行量化评估？

#### 解答：

当密码技术为满足信息系统安全需求提供了机密性、完整性、真实性和/或不可否认性的保护时被正确、有效使用，则“密码使用有效性 D”可判定为“符合”。根据《商用密码应用安全性评估量化评估规则（2023 版）》，在具体量化时，还应进一步考虑密码算法的安全强度，不同安全强度的密码算法在量化评估分值上会有所不同。例如，将密码算法的安全强度分为以下几类：

▶安全强度大于等于 112 比特的密码算法，如 3DES（使用 3 个不同密钥）、AES-128 及以上、SHA-224 及以上、RSA-2048 及以上、ECDSA-P224 及以上、HMAC-SHA1 及以上；

▶安全强度大于等于 80 比特小于 112 比特的密码算法，如 RSA-1024、3DES（使用 2 个不同密钥）、ECDSA-P192；

▶安全强度小于 80 比特的密码算法，DES、MD5、SHA-1、RSA-512。

## 六、风险判定类

### 32.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（2021版）》文件中，部分判定单元中提供了可能的缓解措施，部分判定单元中未提供可能的缓解措施。

### 32.1 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（2021版）》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。

### 32.2 问题：

许多特殊行业的场景（如工控、医疗）不支持直接改造，但依然采用了严格的管理措施来保障风险缓解，高风险判定指引中提到的通用要求和缓解措施无的情况，能否通过严格的管理措施来缓解？

### 解答：

针对特殊行业的场景不支持改造但《信息系统密码应用高风险判定指引（2021版）》中未提供可能的缓解措施的情况，不能直接依据“采用了严格的管理措施”来缓解风险。对于面向互联网的信息系统不支持改造的情况，涉及到的风险建议客观评估。

## 33.应用层身份鉴别是否可以缓解网络层身份鉴别的高风险

## 背景：

“身份鉴别”指标是“网络和通信安全”“应用和数据安全”两个层面的关键性指标。但在实际测评过程中，这两个“身份鉴别”指标可能存在模糊不清、混淆的情况。

## 问题：

“网络和通信安全”“应用和数据安全”的身份鉴别指标有何区别？在测评时如何把握两者的关系？

## 解答：

“网络和通信安全”和“应用和数据安全”的身份鉴别指标的测评对象不同，“网络和通信安全”层面的“身份鉴别”的具体测评对象是客户端与服务器建立的通信信道中的通信实体的身份，应用层身份鉴别的具体测评对象是关键业务应用的用户，因此无法在《商用密码应用安全性评估报告模板（2023版）》的5.1小节进行测评结果修正（也就是无法对测评结果和分值进行“弥补”）。

但在风险评估时，仍应当结合其他层面的“身份鉴别”指标测评结果，对本层面的“身份鉴别”指标和工作机制进行综合考虑，给出合适的风险等级。

例如，“网络和通信安全”对接入的用户设备（服务端鉴别了客户端）进行了身份鉴别，“应用和数据安全”未额外使用身份鉴别机制，而是直接使用了“网络和通信安全”的“身份鉴别”结果，默认接入的用户可以登录应用，此时，“应用和数据安全”身份鉴别指标判定仍为“不符合”，如果网络和通信安全层面接入的用户设备能够表征应用和数据安全层面客户端身份，则可以缓解“应用和数据安全”身份鉴别的风险。

反之亦然，“应用和数据安全”层面对服务端进行了身份鉴别，“网络和通信安全”未采用密码技术实现身份鉴别，在应用和数据安全层面客户端（用户）身份能够表征网络和通信安全层面接入的用户设备身份情况下，可缓解“网络和通信安全”的身份鉴别的风险，“网络和通信安全”身份鉴别指标判定仍为“不符合”。

### 34.如何理解高风险判定指引中的“适用时”

#### 背景：

在《信息系统密码应用高风险判定指引（2021版）》中，网络和通信安全层面、应用和数据安全层面相关高风险项的安全问题中，均涉及了“适用时”。

#### 问题：

在做风险分析和评价时，对于《信息系统密码应用高风险判定指引（2021版）》文件中，部分高风险项的安全问题所提到的“适用时”该如何理解？

#### 解答：

《信息系统密码应用高风险判定指引（2021版）》文件中的“适用时”，是指针对相应指标的密码应用，目前密码产业供给侧存在经检测认证合规的密码产品（即密码产品种类在《商用密码产品认证目录》中）且该密码产品能够满足应用场景实际需求，则视为“适用”。需要注意的是，若密评时判定为“不适用”，则须在密评报告的风险分析环节详细论述原因。

### 35.不涉及高风险的指标使用了高风险算法、技术或产品进行保护时，如何判定风险

#### 背景：

依据《信息系统密码应用高风险判定指引（2021版）》，对于使用了MD5、DES、SHA-1、RSA（不足2048比特）、以及安全性未知的算法等密码算法，SSH1.0、SSL2.0、SSL3.0、TLS1.0等密码技术、存在Heartbleed漏洞的OpenSSL等密码产品时，会导致系统存在高风险安全问题，且无缓解措施。

#### 问题：

《信息系统密码应用高风险判定指引（2021版）》不涉及高风险的指标使用了高风险判定指引中列出的高风险算法、技术或产品，例如二级系

统的网络和通信层面通信数据完整性,但密码套件的完整性算法出现了高风险算法,应如何判定风险。

**解答:**

依据《信息系统密码应用高风险判定指引(2021版)》,在进行风险判定时,应考虑指标实现过程所使用的高风险密码算法、技术或产品是否对风险判定产生影响。

某一特定指标所对应的测评对象,即便在未采用密码技术实施保护措施的情况下,依据风险分析及相关标准判定,其本身也不会形成高风险的话,若该测评对象使用了高风险的算法、技术或产品,建议测评人员还是按照原来的风险等级进行判定。使用的密码算法、技术或产品本身存在的风险等级,不等同于指标项的风险等级。

## 七、特殊场景类

### 36.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。

### 37. 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 39786-2021 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。

#### 37.1 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，测评结论能否复用？

**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（2023版）》中定义的A和K的赋值和适用情况（即，在何种条件下取得相应的量化评估结果；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分析和适用情况（即，在“A”“K”何种条件下相应的风险分析情况，可提供给云上应用在密码应用规划、实施和测评时参考）。

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：

(1) 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，则在云上应用测评时可以复用相关测评对象的测评结论（条件允许时，还应在实际测评时对测评结论加以核实、确认）。

(2) 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。

(3) 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 37-1 被完全评估的支撑能力说明示例**

序	安全	被完全评估的密码支撑能力	测评结果
---	----	--------------	------

号	层面	测评对象	可能涉及的指标	量化评估分值	结果判定	风险等级
1	物理和环境安全	云平台机房	身份鉴别	1	符合	/
2			电子门禁记录数据存储完整性	0.5	部分符合	低
3			视频监控记录数据存储完整性	0.5	部分符合	低
4	网络和通信安全	云平台异地机房之间的通信信道	身份鉴别	0.5	部分符合	中
5			通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性	1	符合	/
6		云服务客户业务应用访问云平台密码服务的通信信道	身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性	1	符合	/
7		远程运维管理设备建立的通信信道	身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性	1	符合	/
8		.....	.....	.....	.....	.....
9	设备和计算安全	云服务器密码机	身份鉴别、远程管理通道安全、系统资源访问控制信息完整性、重要信息资源安全标记的完整性、日志记录完整性、重要可执行程序完整性及来源真实性	1	符合	/
10		堡垒机	身份鉴别	1	符合	/
11			远程管理通道安全	0.25	部分符合	高
12			系统资源访问控制信息完整性、重要信息资源安全标记的完整性、日志记录完整性、重要可执行程序完整性及来源真实性	0	不符合	中
13		.....	.....	.....	.....	.....
14	应用和数据安全	云平台支撑应用（如统一身份认证平台）	访问控制信息完整性	0.5	部分符合	中
15		.....	.....	.....	.....	.....

表 37-2 被部分评估的支撑能力说明示例

序号	支撑能力名称	量化评估和适用条件				风险分析情况和适用条件	
		A	适用条件	K	适用条件	风险等级	适用情况
1	电子签	√	当使用 SM3 和 SM2 算法	√	（可以为	中、低	.....

	章服务		进行电子签章时		“无”)		
		×	(可以为“无”)	×	(可以为“无”)	高	.....
2	时间戳	√	.....	√	.....	中、低	.....
	服务	×	.....	×	.....	高	.....
3	服务器	√	.....	√	.....	中、低	.....
	密码机	×	.....	×	.....	高	.....

### 37.2 问题:

在《商用密码应用安全性评估报告模板（2023 版）》的“被测信息系统基本信息表”中增加了“系统是否依赖不在本系统范围内的云平台运行”，但对于云平台和密码服务平台（此处特指密码服务平台为已独立完成等保定级的系统）分别独立开展密评的情况，租户的密评结论会同时依赖于云平台和密码服务平台，尤其是这种情形的“云密码支撑能力”是在密码服务平台侧的。针对这种情况，云平台和密码服务平台密评时，需额外提供哪些信息作为云上应用密评时的参考资料。

### 解答:

对于该情况，云平台和密码服务平台（特指已独立完成等保定级的系统）在各自密评报告中，除给出系统密评结论外，还需提供“被完全评估的支撑能力说明”“被部分评估的支撑能力说明”。例如，云上应用业务运转在云平台上，云上应用租用第三方云密码服务提供商的密码服务平台。那么，云平台的密评报告需体现“被完全评估的支撑能力说明”，密码服务平台的密评报告需体现“被部分评估的支撑能力说明”。另外，在云上应用密评时，可考虑在密评报告的附录中体现所涉及云平台和密码服务平台的密评结论、被完全评估的支撑能力说明、被部分评估的支撑能力说明。

### 37.3 问题:

如果已经取得符合性密评报告的云平台、密码服务平台超期未复评，是否可以被云上应用复用？

### 解答:

在对租户信息系统进行测评时，云平台、密码服务平台不能提供定期复评的报告，云平台、密码服务平台的早期测评报告不能作为租户信息系统测评依据，仍需对平台侧相关指标进行补充测评。

### 38.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。

### 39.特殊系统的测评对象选取

#### 背景：

现阶段，大量的“纯网络”的信息系统被单独定级，如基础网络系统、骨干网络系统、电子政务外网等网络型信息系统，极端情况下骨干网仅涉及核心路由器、交换机、防火墙等网络基础设备。由于这类系统的核心保护内容通常并非是应用系统和数据，因此其测评与一般的信息系统会有差异。

### 问题：

针对这种纯网络系统，如何开展密评工作？网络和通信安全、设备和计算安全、应用和数据安全层面的测评对象如何选取？

### 解答：

针对这类定级系统，首先可根据其密码应用（或改造）方案、网络安全等级保护测评报告等技术材料确认该系统的边界、密码应用需求以及相应的保护对象。若经确认，网络系统确实有密码应用需求以及相应的保护对象，则可按照 GB/T 39786-2021、GB/T 43206-2023 的相关要求选取适用指标进行测评。应用和数据安全层面可分析是否存在网络管理等相关的应用，若存在可考虑作为应用和数据安全层面的测评对象，重要数据的测评对象需要考虑网络本身相关重要数据，例如网络中存储的用户身份标识信息和用户签约策略数据；设备和计算安全层面的测评对象可能包括重要应用所在应用服务器、数据库及数据库服务器、密码产品、堡垒机等；网络和通信安全层面的测评对象可根据信息系统网络连接情况，从通信主体和网络类型这两个方面进行确定，包括跨安全边界的外联通信信道，如网络相关系统与业务运营支撑(计费)系统之间的通信信道。另外，用户侧系统涉及的重要数据不在测评范围内，只用于转发用户数据的用户侧通道可不列为网络与通信安全层面测评对象。

如果单独定级的网络系统仅涉及核心路由器、交换机、防火墙等网络基础设备且不含有任何应用，可将应用和数据安全层列为“不适用”，其他层面仍依据 GB/T 39786-2021、GB/T 43206-2023 以及现有的密评指导性文件开展商用密码应用安全性评估。

## 40.如何开展信息系统密码应用成熟度极低情况下的密码应用管理测评

### 背景：

在对一些密码应用成熟度极差的存量信息系统密评时发现，被测系统除涉及口令通过计算杂凑值（代码实现）进行传输/存储保护或设备远程管理使用 SSH 协议外，未部署任何密码产品或未使用其他任何密码技术对被测系统业务进行安

全防护，因此被测单位未按照 GB/T 39786-2021 中密码应用管理要求落实。

**问题：**

针对部分存量信息系统自身密码应用成熟度极低，未部署任何密码产品对其业务进行密码安全防护，而导致密码应用管理方面无法配套建设的情形，在测评时该如何把握？

**解答：**

针对上述信息系统密码应用成熟度很低的情况，在密评时仍需将 GB/T 43206-2023 中管理制度、人员管理、建设运行和应急处置四个方面纳入测评内容。测评过程中需要进一步考察这四个层面相关制度文件与实际结合情况，如果存在相关制度文件满足指标要求情况，但实际信息系统并未落实密码应用岗位的人员、密码软硬件部署和相应密钥管理等密码应用相关内容时，对应测评单元结果判定时最高为“部分符合”。例如，被测单位虽已建立从业人员上岗培训制度，且明确了密码操作与管理人员的培训内容，但实际未设置对应密码操作、管理岗位，或相关人员上岗前未完成该专项培训，此种情形不能判定为“符合”。

注意：如果在被测信息系统基本无密码应用情况下已制定了密码相关制度和操作规程等内容，在系统密码应用建设完成后，需重点关注密码相关制度和操作规程等文件的适用性情况，核实是否与系统实际情况相符。

#### 41.特定行业或具有特殊密码应用需求的信息系统测评

**背景：**

随着密评工作的普及和深入，部分行业根据自身特点制定了行业标准作为支撑，以规范和指导行业信息系统密码应用建设和密评工作的实施；部分系统责任单位根据自身业务场景和安全目标，提出了信息系统的特殊密码应用需求。针对特定行业或具有特殊密码应用需求的信息系统，无法仅依据 GB/T 39786-2021、GB/T 43206-2023 以及现有的密评指导性文件开展测评方案编制、现场测评、量化评估与风险分析等工作。

## 问题：

特定行业的密码应用标准规范与 GB/T 39786-2021 不一致时（存在特殊指标时）应如何确定测评指标、进行量化评估与风险判定？

## 解答：

测评指标包括基本指标和特殊指标，基本指标依据国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》根据信息系统相应等级决定，特殊指标可能包括 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》未覆盖（如行业标准）或者高于 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中被测系统相应等级的安全要求。

需要注意的是，特殊指标与基本指标类似，参考 GB/T 43206-2023 及其相关标准进行测评，对被测系统在特殊指标方面的表现给出“符合”、“部分符合”或“不符合”的结论；并对其可能带来的安全风险进行全面、深入的风险评价，给出“高”“中”“低”的风险评价，但特殊指标不参与量化评估环节。特殊指标的风险分析结果可能影响整体测评结论。

原则上，行业标准不应与 GB/T 39786-2021 相抵触。GB/T 39786-2021 是信息系统密码应用的基础性标准，为各行业、各类信息系统的密码应用提供了通用性、基础性的要求和指导，也为各行业制定密码应用规范提供了参考框架；各行业可根据自身特点，在 GB/T 39786-2021 的基础上制定更具体的行业标准。行业标准在制定过程中，通常需要与 GB/T 39786-2021 保持一致，在基本要求的基础上进行细化和补充，增加行业的特殊要求，或提出更严格的安全要求。如果确实存在行业标准中的密码应用要求低于 GB/T 39786-2021 的情形，应按照 GB/T 39786-2021 中相应要求开展信息系统的密码应用建设与安全性评估。

以上内容若与最新的密码管理政策不一致的，应以密码管理部门的最新政策为准。