

图解 商用密码应用安全性评估

2024版 V2.0.0

炼石网络

2024年2月



并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

炼石整理：密评相关法规政策一览

	网络安全法	密码法	数据安全法	个人信息保护法
法律	第十二届全国人民代表大会常务委第二十四次会议通过，2017年6月1日起施行	第十三届全国人民代表大会常务委第十四次会议通过，2020年1月1日起施行	第十三届全国人民代表大会常务委第二十九次会议通过，2021年9月1日起施行	第十三届全国人民代表大会常务委第三十次会议通过，2021年11月1日起施行
法规政策	本次解读 商用密码管理条例 (2023年正式稿) 国务院，2023年7月1日施行	商用密码应用安全性评估管理办法 (试行) 国家密码管理局，2017年发布	商用密码应用安全性评估机构管理办法 (试行) 国家密码管理局，2017年9月27日发布	商用密码应用安全性评估机构能力评定实施规范 (试行) 国家密码管理局，2017年9月27日发布
国标	国家密码管理局，2021年发布 本次解读 信息安全技术 信息系统密码应用基本要求 GB/T 39786-2021，国家市场监督管理总局、国家标准化管理委员会发布	国家密码管理局，2007年11月27日发布 本次解读 信息安全技术 信息系统密码应用设计指南 GB/T 43207-2023	国家密码管理局，2023年6月9日发布 本次解读 信息安全技术 信息系统密码应用测评要求 GB/T 43206-2023	国家密码管理局，2023年6月9日发布 本次解读 信息安全技术 信息系统密码应用测评要求 GB/T 43206-2023
行标	信息安全技术 信息系统密码应用基本要求 GM/T 0054-2018，国家密码管理局发布	信息安全技术 信息系统密码应用测评过程指南 GM/T 0116-2021，国家密码管理局发布	密码术语 GM/T 0001-2013，国家密码管理局发布	
团标	本次解读 信息系统密码应用方案评估规范 T/GDCCA 0001-2022，广东省商用密码协会发布	本次解读 信息系统密码应用方案评估过程指南 T/GDCCA 0002-2022，广东省商用密码协会发布		虚线框中文件是相较炼石2023年2月发布的版本，本次解读中有更新的标准/文件
指导性文件	机构 商用密码应用安全性评估机构能力要求和评价规范（报批稿） 商用密码应用安全性评估监督检查规范（送审稿） 管理 信息安全系统密码安全管理规范（送审稿） 工业控制系统密码应用技术要求（送审稿）	人员 密码技术应用国家职业技能标准（征求意见稿） 人力资源社会保障部，2021年9月23日发布 实施 信息安全等级保护商用密码技术实施要求 国家密码管理局，2009年发布 信息系统密码应用实施指南（报批稿）	测评 政务信息系统密码应用与安全性评估工作指南 密评联委会，2020年9月24日发布 本次解读 商用密码应用安全性评估报告模板（2023版） 密评联委会，2023年1月20日发布 本次解读 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，2021年12月17日发布	商用密码应用安全性评估行业自律公约 密评联委会，2021年发布 本次解读 商用密码应用安全性评估量化评估规则（2023版） 密评联委会，2023年7月17日发布 本次解读 商用密码应用安全性评估FAQ（第三版） 密评联委会，2023年10月26日发布

本文总体结构及参考文献

一. 密评背景介绍

- 1 商用密码条例解读
- 2 密评发展历程回顾
- 3 密评开展政策依据

商用密码检测机构管理办法



商用密码应用安全性评估管理办法



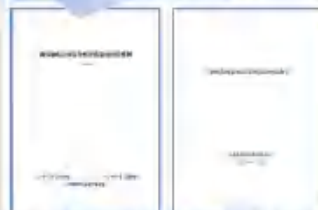
二. 密评总体要求

- 1 测评要求
- 2 评估内容
- 3 密评流程
- 4 高风险项
- 5 测评结论

GB/T 39786-2021信息安全技术 信息系统密码应用基本要求



商用密码应用安全性评估 量化评估规则（2023版）



信息系统密码应用

三. 密评测评要求

- 1 测评要求
- GB/T43206-2023 信息安全技术
信息系统密码应用测评要求



四. 密评方案要求

- 1 技术要求
- GB/T43207-2023 信息安全技术
信息系统密码应用设计指南



五. 密评测评过程

- 1 测评过程
- 2 对象选择
- 3 测试方法
- 4 密评工具
- 5 评估流程
- 6 方案评估
- 7 测试准备
- 8 方案编制
- 9 现场测评
- 10 报告编制

GB/T43207-2023 信息安全技术 信息系统密码应用设计指南



商用密码应用安全性评估报告模板
报告

六. 密评团标解读

信息系统密码应用方案评估规范



信息系统密码应用方案评估过程指南

七. 密评FAQ解读

商用密码应用安全性评估FAQ （第三版）



八. 密改方案效果

- 1 国密合规场景
- 2 数据安全实战防护场景

01 密评背景介绍

02 密评总体要求

03 密评测评要求

04 密评方案要求

05 密评测评过程

06 密评团标解读

07 密改FAQ解读

08 密改方案实践



更新解读

《商用密码管理条例》

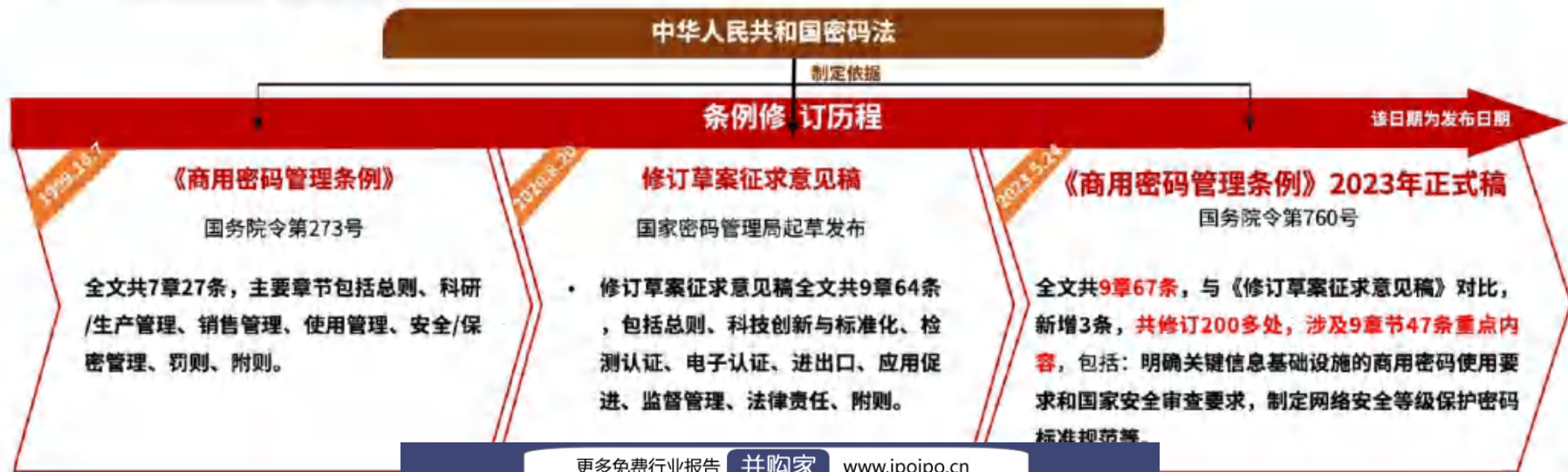
1999年10月7日中华人民共和国国务院令第273号发布
2023年4月27日中华人民共和国国务院令第760号修订

条例概述：规范商用密码应用和管理，发挥密码在网络空间安全中的重要作用



2023年5月24日，中央人民政府网发布2023年4月14日国务院第4次常务会议修订通过的《商用密码管理条例》，《条例》自2023年7月1日起施行，旨在：

规范商用密码应用和管理，鼓励促进商用密码产业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织合法权益。



条例意义：适应新时代商用密码事业发展需求

01 修订必要性

近年来，商用密码应用愈发广泛，在维护国家主权、安全和发展利益以及保障网络和信息安全方面的作用越来越凸显。党的十八大以来，党中央、国务院对商用密码创新发展和行政审批制度改革提出了一系列要求，2020年施行的密码法对商用密码管理制度进行了结构性重塑。为了贯彻落实行政审批制度改革精神，细化密码法相关制度，有必要对原《条例》进行全面修订。

02 总体思路

坚持创新发展与保障安全相结合

在促进商用密码科技创新和科技成果转化的同时，对涉及国家安全、国计民生、社会公共利益的商用密码产品、服务以及关键信息基础设施商用密码应用实施管控

坚持放宽准入与规范监管相结合

按照行政审批制度改革要求，放宽市场准入，由原《条例》规定的全环节严格管控，调整为对关键环节进行重点把控，管理方式由重事前审批转为加强事前事中事后监管，更好激发市场活力社会创造力。

处理好条例与相关法律法规关系

注重与密码法、网络安全法、出口管制法、电子签名法、认证认可条例、关键信息基础设施安全保护条例等做好衔接，并将实践中成熟有效的做法上升为条例规定。

03 修订发布主要过程

国家密码管理局全面贯彻党中央关于新时代商用密码工作的方针政策和国家“放管服”改革总体要求，认真总结商用密码管理工作成功经验，深入研究商用密码发展新形势、新任务，积极借鉴国外密码管理有益做法，在《密码法》立法过程中同步开展《条例》研究修订工作

2019年10月26日

《密码法》颁布后，**国家密码管理局**依法对《条例》修订所涉及的各项制度进一步细化和研究论证，在与有关部门充分协商并修改完善的基础上形成了征求意见稿

2020年6月至9月

征求意见稿印发各省（区、市）密码管理部门征求意见，征求44家中央和国家机关单位和14家企业意见，并在国家密码管理局门户网站面向社会公开征求意见，充分吸收各方面意见的基础上对征求意见稿进行进一步修改完善，形成修订草案送审稿

2020年10月

修订草案送审稿报送国务院。

2023年5月24日

《商用密码管理条例》经国务院第19次常务会议审议通过，并自2023年7月1日起施行。

条例亮点：六大重点修订应对商密在技术进步和产业发展中出现的新情况新问题

1

促进商用密码科技创新

- 明确加强商用密码人才培养，建立健全商用密码人才发展体制机制和人才评价制度，鼓励和支持密码相关学科和专业建设；
- 建立健全商用密码科学技术创新促进机制，支持商用密码科学技术自主创新，对作出突出贡献的组织和个人按照国家有关规定予以表彰和奖励；
- 鼓励支持商用密码科学技术成果转化和产业化应用，建立和完善商用密码科学技术成果信息汇交、发布和应用情况反馈机制；
- 优化现行商用密码科研成果审查鉴定审批的适用范围，依法保护商用密码领域的知识产权；
- 规范商用密码标准的制定、实施、监督、国际化以及法律效力。

2

商用密码检测、认证

- 修订后的《条例》**取消了**原《条例》设置的商用密码产品生产单位审批、商用密码产品销售单位许可、商用密码产品品种和型号审批，实行商用密码检测认证制度。
《条例》规定：
- 一是推进商用密码检测认证体系建设，鼓励在商用密码活动中自愿接受商用密码检测认证；
- 二是明确商用密码检测、认证机构资质审批条件、程序及其从业规范；
- 三是对涉及国家安全、国计民生、社会公共利益的商用密码产品与使用网络关键设备和网络安全专用产品的商用密码服务实行强制性检测认证制度。

3

电子认证

- 《条例》为加强电子认证服务使用密码和电子政务电子认证服务活动管理；
- 一是明确电子认证服务使用密码要求和规范；
- 二是明确电子政务电子认证服务机构的资质审批条件、程序及其从业规范；
- 三是明确建立电子认证信任机制，推动电子认证服务互信互认；
- 四是明确政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务要求。

条例亮点：六大重点修订应对商密在技术进步和产业发展中出现的新情况新问题

4

进出口管理的体制机制

- 为规范商用密码进出口管理，根据密码法关于商用密码进出口的规定以及国家出口管制、两用物项进出口管理制度，《条例》明确：
- 涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制；
- 国务院商务主管部门会同国家密码管理部门和海关总署制定商用密码进口许可清单和出口管制清单；
- 大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

5

促进商用密码应用的规定

- 《条例》坚持总体国家安全观，统筹发展和安全
- 一方面，鼓励公民、法人和其他组织依法使用商用密码保护网络与数据安全，支持网络产品和服务使用商用密码提升安全性，规范商用密码在信息领域新技术、新业态、新模式中的应用。
- 另一方面，明确关键信息基础设施的商用密码使用要求，并加强与国家安全审查、网络安全等级保护制度的衔接。

6

商用密码监管要求

- 为了贯彻落实行政审批制度改革精神，加强事前事中事后监管，《条例》规定了密码管理部门和有关部门的商用密码监督管理职责权限；
- 明确建立商用密码监督管理协作机制，推进商用密码监督管理与社会信用体系相衔接；
- 明确密码管理部门和有关部门及其工作人员不得要求商用密码科研、生产、销售、服务、进出口等单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息，并对其在履行职责中知悉的商业秘密和个人隐私严格保密。

《商用密码管理条例》总结构

商用密码管理条例

第一章 总则

- 1.目的
- 2.适用范围和关键定义
- 3.监管机构
- 4.人才培养
- 5.宣传教育
- 6.学术和行业自律/政府支持

第二章 科技创新与标准化

- 7.创新促进机制/知识产权保护/鼓励外商投资合作
- 8.成果转化机制
- 9.审查鉴定机制
- 10.标准制定
- 11.强制性和推荐性标准

第九章 附则

- 67.条例施行日期

第三章 检测认证

12. 商密检测认证体系
13. 商密检测认证机构资质认定
14. 检测资质取得条件
15. 检测机构资质申请流程
16. 商密检测实施要求
17. 商密认证制度
18. 商密认证机构能力要求
19. 商密认证实施要求
20. 网络关键设备和网络安全专用产品目录
21. 网络关键设备和网络安全专用产品使用要求

第四章 电子认证

22. 能力要求
23. 密码使用要求
24. 服务机构资质认定
25. 认证资质取得条件
26. 电子政务电子认证服务机构资质申请流程
27. 外商投资安全审查
28. 电子政务电子认证机构服务要求
29. 电子认证信任机制
30. 电子签名法律效力

第五章 进出口

31. 商用密码进口许可、出口管制清单
32. 进出口许可证
33. 报关要求
34. 进出口许可申请材料及流程

第八章 法律责任

50. 未经认证的商密检测或电子认证服务处罚
51. 商密检测机构违法行为处罚
52. 商密认证机构违法行为处罚
53. 销售/提供未经检测认证或不合格的产品/服务处罚
54. 电子认证服务机构违反法律和密码技术规范的处罚
55. 电子政务电子认证服务机构处罚
56. 电子政务电子认证服务机构无法自证的承担赔偿责任
57. 政务活动中不合规的电子认证处罚
58. 进出口商密的处罚
59. 窃取加密信息、非法入侵商密系统违法行为处罚
60. 关基运营者违法处罚
61. 关基运营者使用未安全审查的产品/服务的处罚
62. 网络运营者处罚
63. 阻挠商密监督管理的处罚
64. 国家机关违法行为处罚
65. 密码管理部门和工作人员的处罚
66. 刑事责任、民事责任

第六章 应用促进

35. 鼓励各主体依法使用密码
36. 支持网络产品和服务使用商密应用
37. 应用促进协调机制
38. 关基运营要求
39. 关基运营产品/服务使用要求
40. 关基运营者采购商密产品和服务的安全审查机制
41. 网络运营者等关基运营/制定网络安全等级保护密码标准规范
42. 测评、关基测评、等级测评衔接避免重复评估

第七章 监督管理

43. 监督检查职责
44. 监督管理协作机制
45. 监督检查职权
46. 信用记录、监督、惩戒、修复机制
47. 保密义务
48. 商密监督管理
49. 举报机制

补充了商用密码应用安全性评估的相关图解内容

商用密码应用安全性评估对采用商用密码技术、产品和服务集成建设的网络和信息系统的密码应用的合规性、正确性、有效性进行评估，是商用密码产业健康发展的“监督员”。

炼石围绕《商用密码管理条例》的具体内容，以图文形式深入浅出解析了条例要点的同时，并从商用密码应用的角度出发，补充了商用密码应用安全性评估的相关图解内容，以更好展示商用密码管理和应用的相关知识。内容供读者学习参考，不足之处诚邀大家共同完善。

明确商用密码定义与各层级监管部门职责

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

8.法律责任

9.附 则

适用范围

在中华人民共和国境内的商用密码科研、生产、销售、服务、检测、认证、进出口、应用等活动及监督管理，适用本条例。

重要定义

商用密码

是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

监管部门

坚持中国共产党对商用密码工作的领导，贯彻落实总体国家安全观

国家密码管理部门

负责管理全国的商用密码工作

县级以上地方各级密码管理部门

负责管理本行政区域的商用密码工作

网信

商务

海关

市场监督
管理

.....

在各自职责范围内，负责商用密码有关管理工作

引导各主体加强人才培养、宣传教育及行业自律

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

8.法律责任

9.附 则



人才培养

国家加强商用密码人才培养，建立健全商用密码人才发展体制机制和人才评价制度，鼓励和支持密码相关学科和专业建设，规范商用密码社会化培训，促进商用密码人才交流。



宣传教育

各级人民政府及其有关部门应当采取多种形式加强商用密码宣传教育，增强公民、法人和其他组织的密码安全意识。



学术和行业自律

商用密码领域的学会、行业协会等社会组织依照法律、行政法规及其章程的规定，开展学术交流、政策研究、公共服务等活动，加强学术和行业自律，推动诚信建设，促进行业健康发展。
密码管理部门应当加强对商用密码领域社会组织的指导和支持。

落实多项机制提升商密技术创新、知识产权保护及成果转化能力

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

8.法律责任

9.附 则

01 创新促进机制

国家建立健全商用密码科学技术创新促进机制，支持商用密码科学技术自主创新，对作出突出贡献的组织和个人按照国家有关规定予以表彰和奖励。

02 知识产权保护机制

国家依法保护商用密码领域的知识产权。从事商用密码活动，应当增强知识产权意识，提高运用、保护和管理知识产权的能力。

03 鼓励在外商投资合作

国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

04 成果转化机制

国家鼓励和支持商用密码科学技术成果转化和产业化应用，建立和完善商用密码科学技术成果信息汇交、发布和应用情况反馈机制。

05 安全审查机制

国家密码管理部门组织对法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统所使用的密码算法、密码协议、密钥管理机制等商用密码技术进行审查鉴定。

科技创新与成果转化

加快商用密码行业标准、国家标准及国际标准制定进程

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

8.法律责任

9.附 则

01 规范、引导和监督标准制定

- 依据各自职责，组织制定商用密码国家标准、行业标准，对商用密码团体标准的制定进行规范、引导和监督，国家密码管理部门依据职责。建立商用密码标准实施信息反馈和评估机制，对商用密码标准实施进行监督检查。
- 其他领域的标准涉及商用密码的，应当与商用密码国家标准、行业标准保持协调。

02 推动国际标准化活动

国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用，鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。



03 强制性和推荐性标准遵循

- 从事商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准，以及自我声明公开标准的技术要求。
- 国家鼓励在商用密码活动中采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

国家鼓励在商用密码活动中自愿接受商用密码检测认证

1.总 则

国家

- 推进商用密码技术**检测认证体系建设**，鼓励在商用密码活动中**自愿接受**商用密码检测认证。

2.科技创新与标准化

国家密码管理部门

- 商用密码**检测技术规范、规则**由国家密码管理部门制定并公布。

4.电子认证

国务院市场监督管理部门会同国家密码管理部门

5.进出口

- 建立国家统一推行的商用密码认证制度**
- 实行商用密码产品、服务、管理体系认证
- 制定并公布认证目录和技术规范、规则

6.应用促进

关键领域商用密码**产品** 实行**强制性认证**

关键领域商用密码**服务** 实行**强制性认证**

7.监督管理

8.法律责任

- 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的商用密码检测、认证机构

- 商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

9.附 则

明确商用密码检测机构资质审批条件、流程及其从业规范

1.总则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

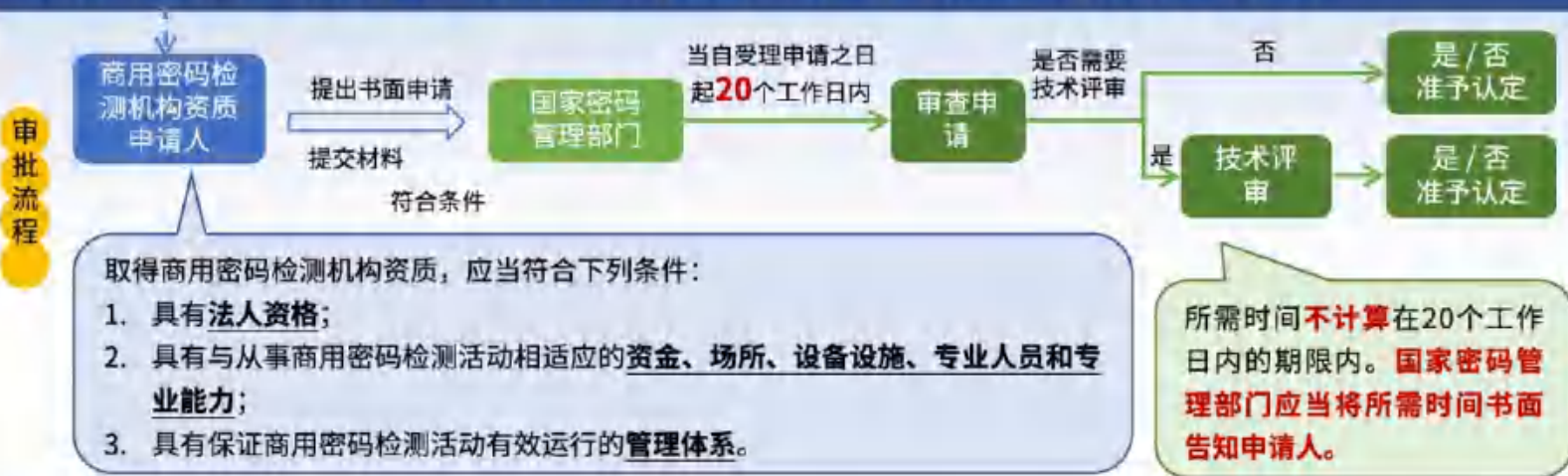
6.应用促进

7.监督管理

8.法律责任

9.附则

从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，面向社会出具具有证明作用的数据、结果的机构，应当经国家密码管理部门认定，依法取得商用密码检测机构资质。



从业规范

- 商用密码检测机构应按照法律、行政法规和商用密码检测技术规范、规则，在批准范围内**独立、公正、科学、诚信**地开展商用密码检测
- **对出具的检测数据、结果负责**
- **定期**向国家密码管理部门报送检测实施情况

明确商用密码认证机构资质审批条件、程序及其从业规范

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

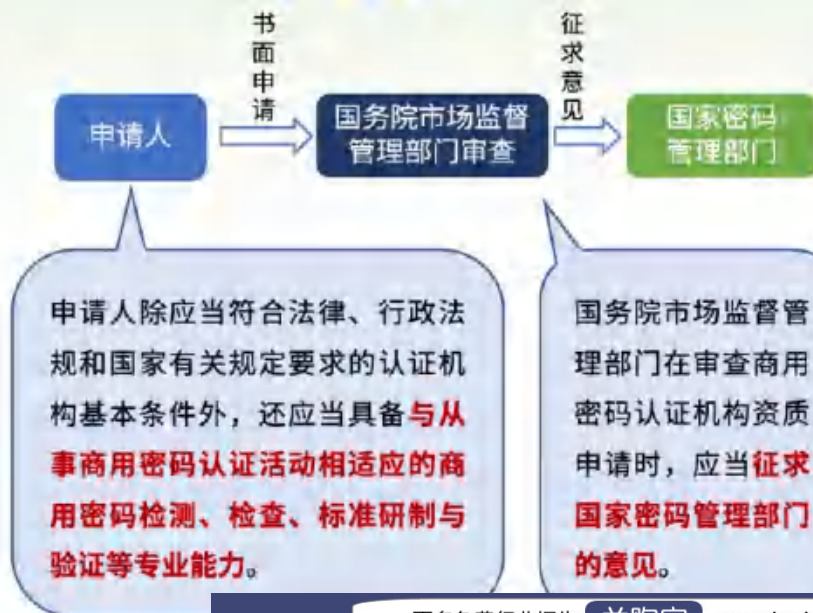
7.监督管理

8.法律责任

9.附 则

从事商用密码认证活动的机构，应当依法取得商用密码认证机构资质。

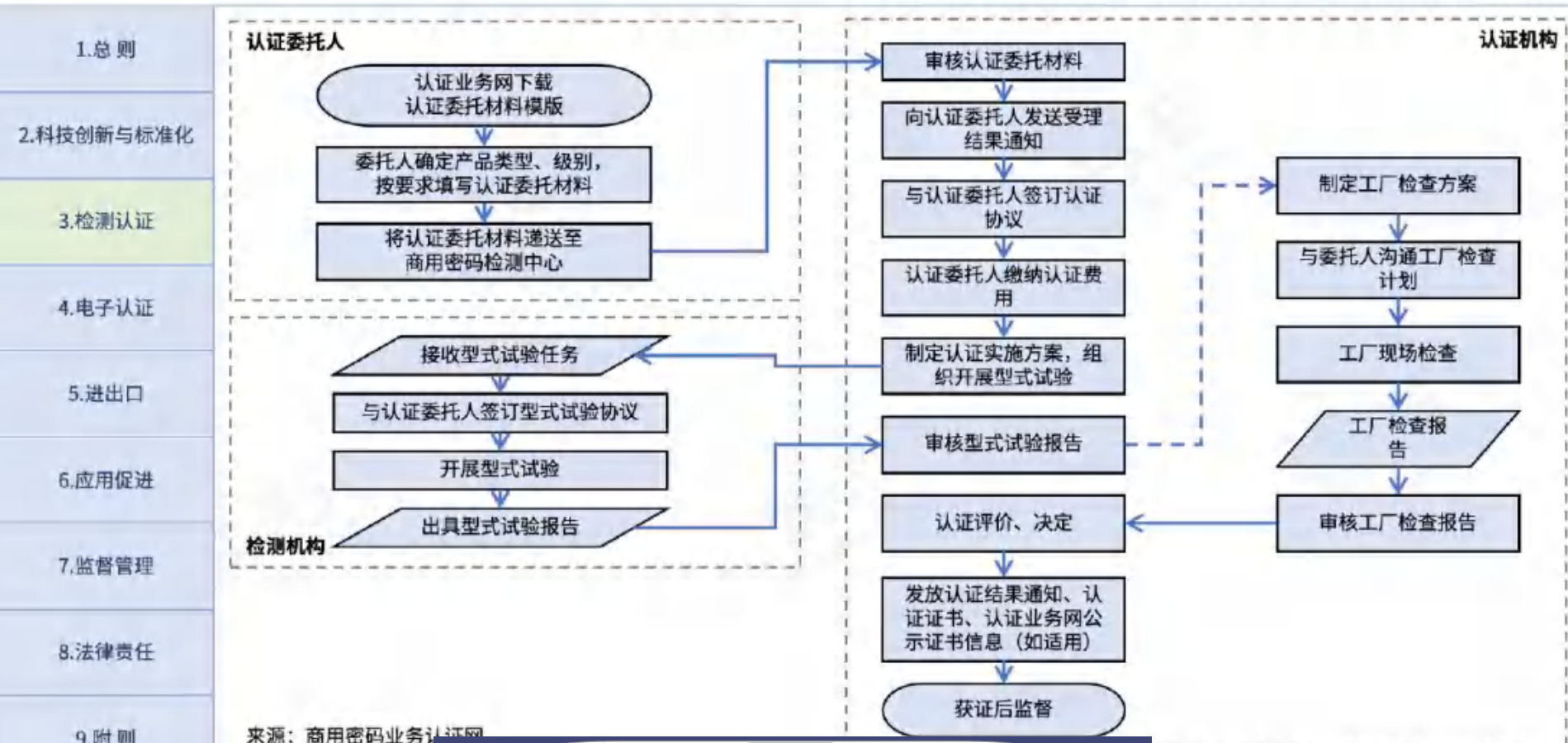
审 批 流 程



从 业 规 范

- 商用密码认证机构应当按照法律、行政法规和商用密码认证技术规范、规则，在批准范围内独立、公正、科学、诚信地开展商用密码认证
- 对出具的认证结论负责
- 对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查，以保证通过认证的商用密码产品、服务、管理体系持续符合认证要求

补充说明：商用密码认证全流程图



明确电子认证服务使用密码要求和使用规范

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

8.法律责任

9.附 则

电子认证服务机构要求

采用商用密码技术 提供电子认证服务要求

- 应当具有与使用密码相适应的场所、设备设施、专业人员、专业能力和管理体系
- 依法取得国家密码管理部门同意使用密码的证明文件

- 应当按照法律、行政法规和电子认证服务密码使用技术规范、规则，使用密码提供电子认证服务，保证其电子认证服务密码使用持续符合要求



电子政务电子认证服务机构的资质审批条件、程序及其从业规范

1.总则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

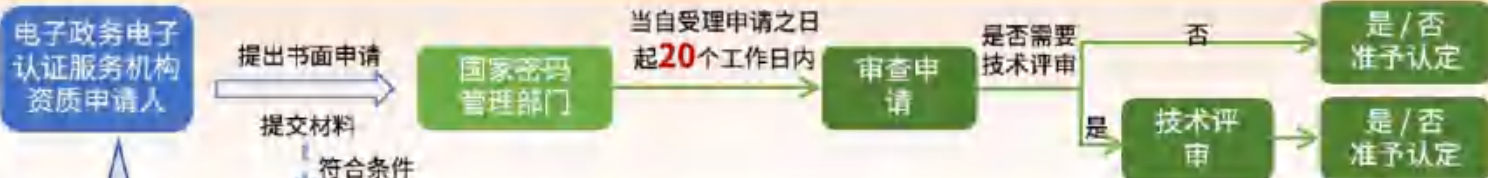
8.法律责任

9.附则

审批流程

从业规范

采用商用密码技术从事电子政务电子认证服务的机构，应当经国家密码管理部门认定，依法取得
电子政务电子认证服务机构资质



取得电子政务电子认证服务机构资质，应当符合下列条件：

1. 具有企业法人或者事业单位法人资格；
2. 具有与从事电子政务电子认证服务活动及其使用密码相适应资金、场所、设备设施和专业人员；
3. 具有为政务活动提供长期电子政务电子认证服务的能力；
4. 具有保证电子政务电子认证服务活动及其使用密码安全运行的管理体系。

所需时间**不计算**在20个工作日内期限内。**国家密码管理部门应当将所需时间书面告知申请人。**

外商投资电子政务电子认证服务

- 影响或者可能影响国家安全的，**应当依法进行外商投资安全审查。**

电子政务电子认证服务机构

- 应当按照法律、行政法规和电子政务电子认证服务技术规范、规则，在批准范围内提供电子政务电子认证服务
- 定期向主要办事机构所在地省、自治区、直辖市密码管

实施情况

国家建立统一的电子认证信任机制

1.总 则	国家
2.科技创新与标准化	建立<u>统一的电子认证信任机制</u>
3.检测认证	国家密码管理部门
4.电子认证	- 负责<u>电子认证信任源的规划和管理</u>，会同有关部门推动电子认证服务互信互认。 <u>电子认证服务密码使用技术规范、规则</u>由国家密码管理部门制定并公布。 <u>电子政务电子认证服务技术规范、规则</u>由国家密码管理部门制定并公布。
5.进出口	密码管理部门会同有关部门
6.应用促进	负责<u>政务活动中使用电子签名、数据电文的管理</u>。
7.监督管理	电子政务电子认证服务机构
8.法律责任	政务活动中的<u>电子签名、电子印章、电子证照</u>等涉及的电子认证服务，应当由依法设立的<u>电子政务电子认证服务机构</u>提供。
9.附 则	

补充说明：我国主要的电子认证服务机构（46家）

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

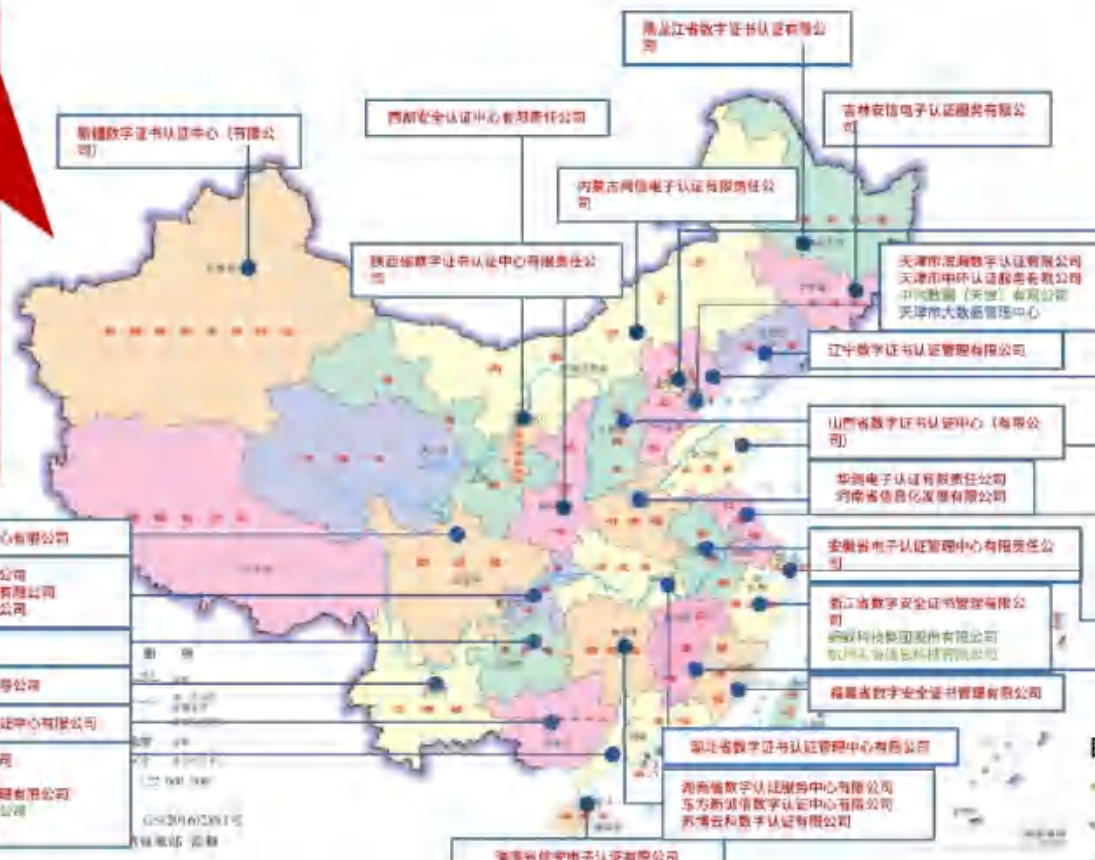
7.监督管理

8.法律责任

9.附 则

根据《电子签名法》《电子认证服务管理办法》《电子认证服务密码管理办法》等法律法规，电子认证服务机构必须按照国家密码主管部门的要求提供相关服务，接受主管部门的安全性审查和运营服务的监督检查，并需要同时取得国家密码管理局颁发的《电子认证服务使用密码许可证》及工业和信息化部颁发的《电子认证服务许可证》，方能对外开展电子认证服务。

四川省数字证书认证管理中心有限公司
东方中讯数字证书认证有限公司
重庆致远未来电子签名服务有限公司
大城云盾电子认证服务有限公司
贵州省数字证书有限公司
云南省数字证书认证中心有限公司
广西壮族自治区数字证书认证中心有限公司
广东省电子商务认证有限公司
数安时代科技股份有限公司
深圳市电子商务安全证书管理有限公司
深圳站网技术（深圳）有限公司
沃通电子认证服务有限公司



中金金融认证中心有限公司
北京天威诚信电子服务有限公司
北京数字认证股份有限公司
网信科技有限公司
北京市信息安全电子认证有限公司
福建数字安全科技有限公司
北京中认环宇信息安全技术有限公司
中信信安（北京）软件有限公司
北京世纪互联网络科技股份有限公司
赛尔认证中心
中信信安咨询有限公司有限公司
中国电力科学研究院有限公司
国网（北京）智能电网有限公司
北京中网通信智能电网技术有限公司
北京鑫源科技有限公司
教育部教育管理信息中心
交通运输部公路科学研究所
人力资源和社会保障部信息中心
国家信息中心
中国电子口岸数据中心
国家商务办公机关服务中心
河北省电子认证有限公司
山东省数字证书认证管理有限公司
山东鑫安安全认证服务有限公司
山东信安认证服务有限公司
南京数字认证有限公司
江苏省国信科技股份有限公司
江苏智慧数字认证有限公司
江苏国盾数字认证有限公司
江苏公信数信数字认证有限公司
江苏省电子政务服务认证中心
上海市数字认证中心有限公司
上海信安科技（上海）有限公司
江西省数字证书有限公司

图 例：

- 电子认证服务使用密码许可单位
- 电子政务电子认证服务机构
- 同时兼具以上两者

商用密码进出口需确认是否属于进口许可或出口管制范围

1. 总则

2. 科技创新与标准化

3. 检测认证

4. 电子认证

5. 进出口

6. 应用促进

7. 监督管理

8. 法律责任

9. 附则



关于时限限制：对国家安全、社会公共利益或者外交政策有重大影响的商用密码出口，由国务院商务主管部门会同国家密码管理部门等有关部门报国务院批准。**报国务院批准的，不受前款规定时限的限制。**

关于进口许可和出口管制清单：涉及国家安全、社会公共利益且具有加密保护功能的商用密码，列入《商用密码进口许可清单》，实施进口许可。涉及国家安全、社会公共利益或者中国承担国际义务的商用密码，列入《商用密码出口管制清单》，实施出口管制。

《商用密码进口许可清单》和《商用密码出口管制清单》

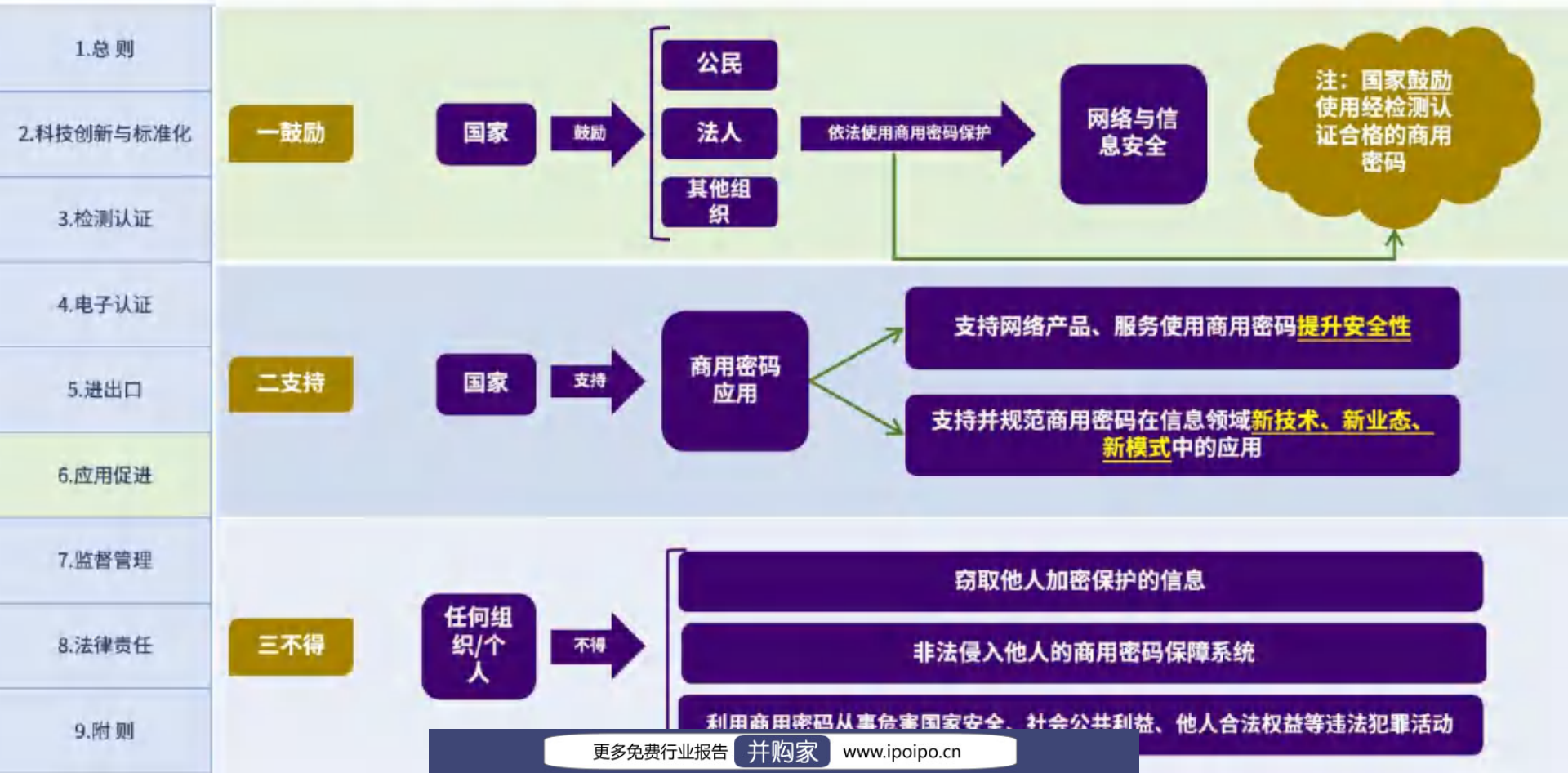
更多免费行业报告

并购家

www.ipopo.cn

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

国家鼓励支持商用密码的规范应用



国家建立商用密码应用促进协调机制

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

5.进出口

6.应用促进

7.监督管理

8.法律责任

9.附 则



关键信息基础设施需使用商用密码进行保护

	义务主体	义务简介	具体要求
1.总 则	法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施的运营者	使用商用密码进行保护	其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。
2.科技创新与标准化		制定商用密码应用方案	
3.检测认证		同步规划、同步建设、同步运行商用密码保障系统	网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级，确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。
4.电子认证		按照国家网络安全等级保护制度要求，使用商用密码保护网络安全	
5.进出口		运行后每年至少进行一次评估	
6.应用促进		商用密码技术应当通过国家密码管理部门审查鉴定	关键信息基础设施通过商用密码应用安全性评估方可投入运行，运行后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。
7.监督管理			使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。
8.法律责任			商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接，避免重复评估、测评。
9.附 则		特殊情况：关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。	

更多免费行业报告 并购家 www.ipoiipo.cn

建立协作机制，加强商密检察、指导、监督工作

1.总 则

2.科技创新与标准化

3.检测认证

4.电子认证

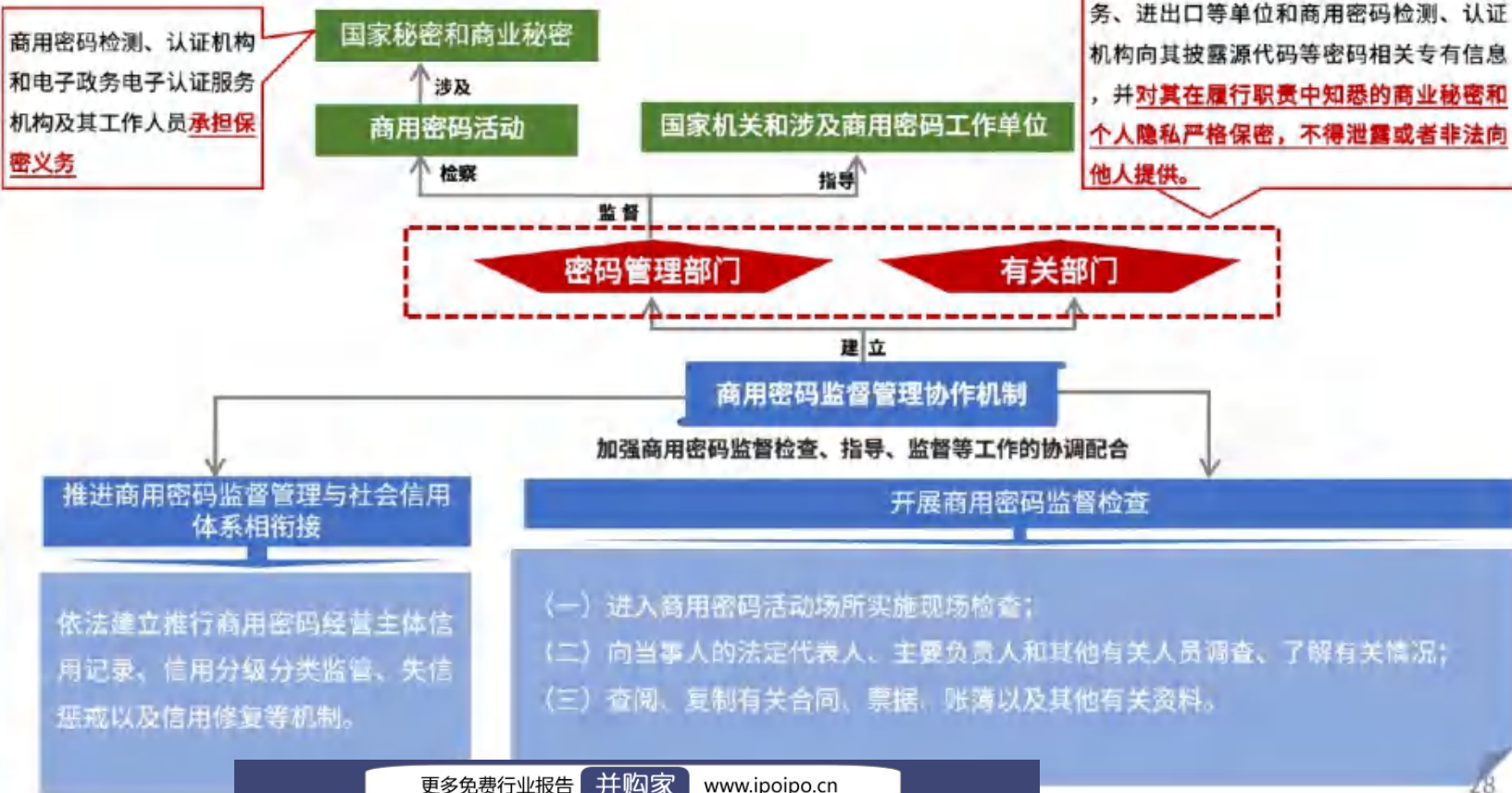
5.进出口

6.应用促进

7.监督管理

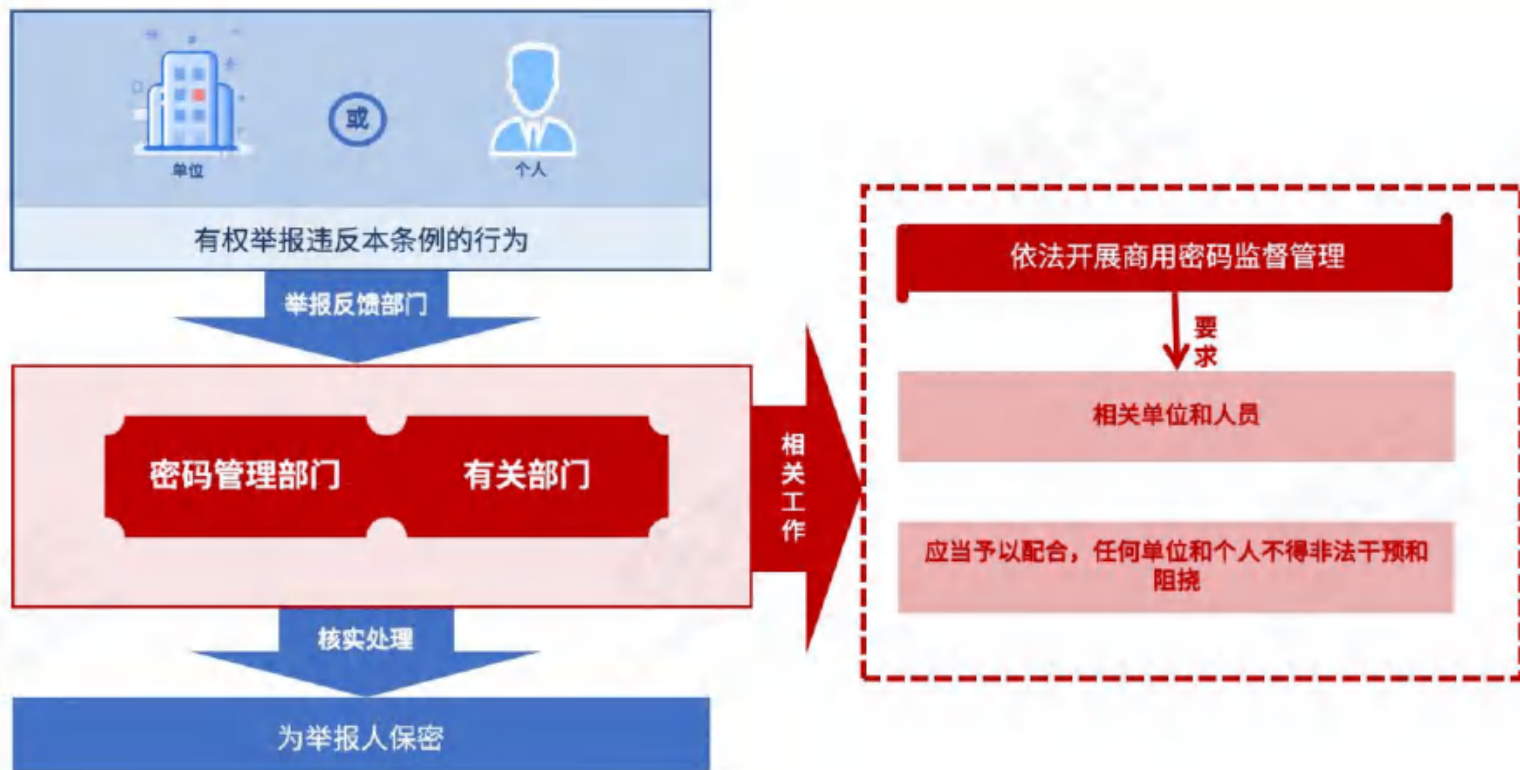
8.法律责任

9.附 则



依照本条例相关要求单位和个人均可举报监督

1.总 则
2.科技创新与标准化
3.检测认证
4.电子认证
5.进出口
6.应用促进
7.监督管理
8.法律责任
9.附 则



违反条例轻者监管部门警告处罚，情节严重者依法承担法律责任

	主体	违法行为	处罚
1.总 则			
2.科技创新与标准化		违反本条例规定， <u>未经认定向社会开展商用密码检测活动，或者未经认定从事电子政务电子认证服务的</u>	<u>由密码管理部门责令改正或者停止违法行为，给予警告</u> ，没收违法产品和违法所得；违法所得30万元以上的，可以并处违法所得1倍以上3倍以下罚款；没有违法所得或者违法所得不足30万元的，可以并处10万元以上30万元以下罚款。
3.检测认证			
4.电子认证		违反本条例第二十条、第二十一条规定， <u>销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证不合格的商用密码服务的</u>	由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得； <u>违法所得10万元以上的，可以并处违法所得1倍以上3倍以下罚款</u> ；没有违法所得或者违法所得不足10万元的，可以并处3万元以上10万元以下罚款。
5.进出口	企业或机构		
6.应用促进		违反本条例规定， <u>未经批准从事商用密码认证活动</u>	由市场监督管理部门会同密码管理部门依照前款规定予以处罚。
		违反本条例规定进出口商用密码	由国务院商务主管部门或者海关依法予以处罚。
7.监督管理		违反本条例规定， <u>构成犯罪</u>	依法追究刑事责任
		给他人造成损害的	依法承担民事责任
8.法律责任			
		无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的	处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节特别严重的，责令停业整顿，直至吊销商用密码许可证件。
9.附 则			

违反条例轻者监管部门警告处罚，情节严重者依法承担法律责任

	主体	违法行为	处罚
1.总 则	商用密码检测机构	开展商用密码检测，有下列情形之一的：	由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得30万元以上的，可以并处违法所得1倍以上3倍以下罚款；没有违法所得或者违法所得不足30万元的，可以并处10万元以上30万元以下罚款； 情节严重的，依法吊销商用密码检测机构资质。
2.科技创新与标准化		(一) 超出批准范围；	
3.检测认证		(二) 存在影响检测独立、公正、诚信的行为；	
4.电子认证		(三) 出具的检测数据、结果虚假或者失实；	
5.进出口	商用密码认证机构	(四) 拒不报送或者不如实报送实施情况；	由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得30万元以上的，可以并处违法所得1倍以上3倍以下罚款；没有违法所得或者违法所得不足30万元的，可以并处10万元以上30万元以下罚款； 情节严重的，依法吊销商用密码认证机构资质。
6.应用促进		(五) 未履行保密义务；	
7.监督管理		(六) 其他违反法律、行政法规和商用密码检测技术规范、规则开展商用密码检测的情形。	
8.法律责任		开展商用密码认证，有下列情形之一的：	
9.附 则	电子认证服务机构	(一) 超出批准范围；	由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得30万元以上的，可以并处违法所得1倍以上3倍以下罚款；没有违法所得或者违法所得不足30万元的，可以并处10万元以上30万元以下罚款； 情节严重的，依法吊销电子认证服务使用密码的证明文件。
		(二) 存在影响认证独立、公正、诚信的行为；	
		(三) 出具的认证结论虚假或者失实；	
		(四) 未对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查；	
		(五) 未履行保密义务；	
		(六) 其他违反法律、行政法规和商用密码认证技术规范、规则开展商用密码认证的情形。	
		违反法律、行政法规和电子认证服务密码使用技术规范、规则使用密码的	

违反条例轻者监管部门警告处罚，情节严重者依法承担法律责任

	主体	违法行为	处罚
1.总 则			
2.科技创新与标准化	电子政务电子认证服务机构	开展电子政务电子认证服务，有下列情形之一的 (一) 超出批准范围； (二) 拒不报送或者不如实报送实施情况； (三) <u>未履行保密义务；</u> (四) 其他违反法律、行政法规和电子政务电子认证服务技术规范、规则提供电子政务电子认证服务的情形。	由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得30万元以上的，可以并处违法所得1倍以上3倍以下罚款； <u>没有违法所得或者违法所得不足30万元的，可以并处10万元以上30万元以下罚款；情节严重的，责令停业整顿，直至吊销电子政务电子认证服务机构资质。</u>
3.检测认证			
4.电子认证	电子签名人或者电子签名依赖方	因依据电子政务电子认证服务机构提供的电子签名认证服务在政务活动中遭受损失，电子政务电子认证服务机构不能证明自己无过错的	承担赔偿责任。
5.进出口			
6.应用促进	政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务	违反本条例第三十条规定，未由依法设立的正务政务电子认证服务机构提供的	由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，由密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。有关国家机关、单位应当将处分或者处理情况书面告知密码管理部门。
7.监督管理			
8.法律责任	关键信息基础设施的运营者	违反本条例第三十八条、第三十九条规定，未按照要求使用商用密码， <u>或者未按照要求开展商用密码应用安全性评估的</u>	由密码管理部门责令改正，给予警告； <u>拒不改正或者有其他严重情节的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。</u>
9.附 则		违反本条例第四十条规定， <u>使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的</u>	由有关主管部门责令停止使用，处采购金额1倍以上10倍以下罚款；对直接负责的主管人员和其他直接责任人员处1万元以上10

违反条例轻者监管部门警告处罚，情节严重者依法承担法律责任

1.总 则	主体	违法行为	处罚
2.科技创新与标准化	国家机关	第六十条、第六十一条、第六十二条、第六十三条所列违法情形的	由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，由密码管理部门、有关部门建议有关国家机关对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。有关国家机关应当将处分或者处理情况书面告知密码管理部门、有关部门。
3.检测认证			
4.电子认证			
5.进出口	密码管理部门和有关部门的工作人员	在商用密码工作中滥用职权、玩忽职守、徇私舞弊， 或者 <u>泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的</u>	依法给予处分。
6.应用促进	黑客等不法分子	<u>窃取他人加密保护的信息，非法侵入他人的商用密码保障系统，</u> 或者利用商用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的	<u>由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。</u>
7.监督管理			
8.法律责任	网络运营者	违反本条例第四十一条规定，未按照国家网络安全等级保护制度要求使用商用密码保护网络安全的	由密码管理部门责令改正，给予警告； <u>拒不改正或者导致危害网络安全等后果的，处1万元以上10万元以下罚款，对直接负责的主管人员处5000元以上5万元以下</u>
9.附 则			

新版《商用密码管理条例》施行日期

1.总 则
2.科技创新与标准化
3.检测认证
4.电子认证
5.进出口
6.应用促进
7.监督管理
8.法律责任
9.附 则



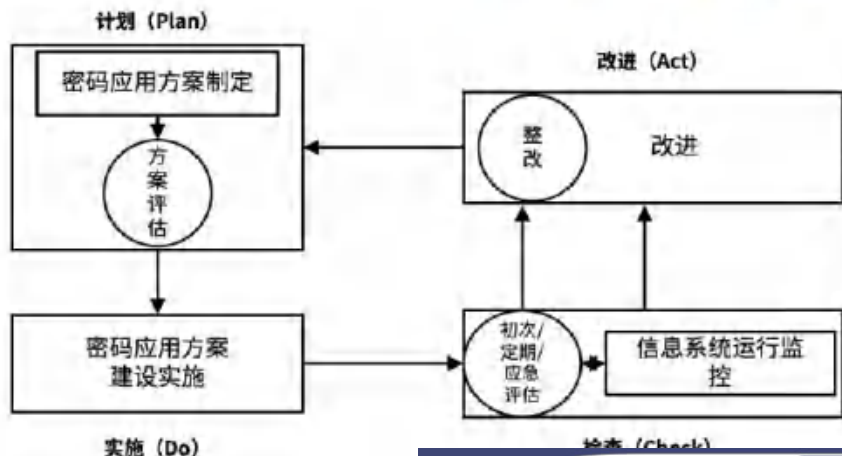
密评发展历程回顾

《密码法》第二十七条规定：运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级保护测评制度相衔接，避免重复评估、测评。

《密码法》第三十七条规定：关键信息基础设施的运营者未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

《“十四五”数字经济发展规划》，明确提出支持开展常态化安全风险评估，加强网络安全等级保护和密码应用安全性评估。

商用密码应用安全性评估，指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的**合规性、正确性、有效性**进行评估。



密评发展历程回顾

推广发展期

2021年起

- “十四五”时期，是数字化引领密评高质量发展重要机遇期，密评加速推广发展。本阶段，密评在金融、政务、教育、电信、水利等行业将实现规模化布局，在评估机制、试点机构规模、技术创新能力、检测认证和标准支撑体系、产业生态环境、产融合作试点、人才队伍建设等方面将形成较强综合竞争力，为数字经济高速发展构建安全屏障。

2017.10-2021

试点开展期

- 2017年10月，商用密码应用安全性评估试点工作开展；2018年2月，国密局经过评审，第一批共有10家测评机构符合测评机构能力要求。
- 2019年上半年，对第一批密评试点做了评审总结，对参与试点的27家机构进行能力再评审，择优选出16家扩大试点，对另11家机构给予6个月的能力提升整改期。
- 2019年10月，开启第二批密评试点工作；2020年7月，评估试点机构增至24家。
- 2021年6月，国家密码管理局第42号公告，发布最新的《商用密码应用安全性评估试点机构目录》，明确48家商用密码应用安全性评估试点机构。

体系建设期

2017.5-2017.9

- 国密局成立密评领导小组，确定密评体系总体架构，起草14项制度文件。
- 2017年9月27日，国密局印发《商用密码应用安全性测评机构管理办法（试行）》等，密评制度体系初步建立。

2016.9-2017.4

再次集结期

2016-2021

试点建设期

- 国密局成立起草小组，起草《商用密码应用安全性评估管理办法（试行）》。
- 2017年4月22日，国密局印发《关于开展密码应用安全性评估试点工作的通知》（国密局（2017）138号文）在七省五行业开展密评试点。

制度奠基期

- 2007年11月27日，国家密码管理局印发11号文件《信息安全等级保护商用密码管理办法》，要求信息安全等级保护商用密码测评工作由国家密码管理局指定的测评机构承担。
- 2009年12月15日，国家密码管理局印发管理办法，明确与密码测评有关的要求。

密码法

第一章 总则

1. 立法目的
2. 密码定义
3. 坚持总体国家安全观
4. 统一领导
5. 分级负责
6. 分类管理
7. 核心密码、普通密码管理
8. 商用密码管理
9. 创新发展、人才建设
10. 密码安全教育
11. 纳入规划和经费预算
12. 禁止行为

第二章 核心密码、普通密码

13. 管理原则
16. 工作监督检查
19. 提供免检便利

14. 使用要求

17. 安全协作机制和问题查处

20. 建立安全审查制度

第三章 商用密码

21. 管理原则
24. 标准法律效力
27. 关基使用要求
30. 行业协会职责

22. 标准体系

25. 检测认证

28. 进口许可和出口管制

31. 事中事后监管和保密义务

15. 安全保密管理

18. 工作机构和人员管理

23. 国际标准化

26. 产品和服务市场准入管理

29. 电子政务电子认证服务

第四章 法律责任

32. 从事密码违法活动追责
33. 核心、普通密码违法使用处罚
34. 核心、普通密码泄密等处罚
35. 商用密码检测、认证违法处罚
36. 商用密码市场准入违法处罚
37. 关基运营者处罚
38. 进出口处罚
39. 电子政务电子认证服务处罚
40. 密码管理部门工作人员处罚
41. 刑事责任、民事责任

第五章 附则

42. 密码管理规章

43. 解放军和武警部队密码立法

44. 施行时间

数据安全法

第一章 总则

1.立法目的

2.适用范围

3.定义

4.坚持总体国家安全观

5.协调机制

6.部门职责

7.基本权利

8.基本义务

9.共同维护

10.行业自律

11.国际合作

12.投诉举报

第二章 数据安全与发展

13.
产业发展

14.
大数据战略

15.
老年人残疾人权益

16.
技术研究

17.
标准体系

18.
检测认证服务

19.
数据交易管理制度

20.
人才培养

第四章 数据安全保护义务

27.主要责任

28.价值取向

29.监测处置

30.风险评估

31.数据出境

32.收集数据禁则

33.交易中介责任

34.行政许可前置

35.执法调取数据

36.跨境司法合作

第五章 政务数据的安全与开放

37.
推行电子政务建设

38.
国家机关依法收集数据

39.
保护政务数据安全

40.
委托建设电子政务系统要求

41.
政务数据公开

42.
政务数据开放目录

43.
公共事务组织的适用

第六章 法律责任

44.针对数据处理风
险约谈整改

45.关于数据安全保
护义务罚则

46.
关于数据出境罚则

47.
交易中介罚则

48.
关于数据调取罚则

49.对国家机关罚则

50.
对国家人员的罚则

51.非法获取数据、
限制竞争等罚则

52.
民事刑事责任

第三章 数据安全制度

21.
分类分级

22.
风险评估、报告、信息
共享、监测预警

23.
应急处置

24.
数据安全审查

25.
出口管制

26.
对等反制

第七章 附则

53.涉密、统计档案、个人信息保护的他法遵循

54.军事数据安全保护的他法遵循

55.施行时间

《个人信息保护法》总结构

个人信息保护法

第一章 总则

第二章 个人信息处理规则

第六章 履行个人信息保护职责的部门

1.目的

2.宗旨

3.适用范围

4.关键定义

5.基本原则

6.目的、必要

7.公开、透明

8.准确、完整

9.责任到人

10.禁止行为

11.环境构建

12.国际合作

第一节 一般规定

13.处理前提

14.取得同意

15.撤回同意

16.不得拒绝服务

17.告知要求

18.例外情形

19.存储期限

20.共同处理

21.委托处理

22.信息转移

23.第三方共享

24.自动化决策

25.不得公开

26.公共聚集

27.处理公开信息

第二节 敏感个人信息的处理规则

第三节 国家机关处理个人信息的特别规定

28.关键定义

29.单独同意

30.必要性告知

31.未成年人保护

32.行政许可

33.适用范围

34.范围限度

35.告知同意

36.境内存储

37.对管理公共事务组织的义务

第三章 个人信息跨境提供的规则

38.前提条件

39.告知要求

40.关基等要求

41.主管批准

42.限制清单

43.对等反制

第四章 个人在个人信息处理活动中的权利

第五章 个人信息处理者的义务

44.知情、决定

45.查阅、复制

46.更正、补充

51.基本义务

52.责任到人

53.境外机构义务

47.主动删除

48.解释说明

49.近亲属行权

54.合规审计

55.影响评估

56.评估内容

50.处理机制

57.补救通知

58.特殊类型个人信息处理者义务

59.受托人义务

第七章 法律责任

第八章 附则

66.行政责任

67.信用档案

68.国家机关处罚

72.特殊情况

73.专业术语

74.施行时间

69.民事责任

70.公益诉讼

71.行政、刑事责任

密评等保相互衔接

		密评	等保
联系		- 密评对象主要包含法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施等； - 等保测评对象基本涵盖了全部的网络和信息系统，第三级以上的网络安全等级保护对象一般也是关基和密评的评估对象； - 关键基础设施是等保测评和密评共同的评估对象。	
区别	评测目的	针对信息系统密码应用的合规性、正确性、有效性进行评估	对信息系统网络安全防护能力进行测评
	评估内容	- 技术要求：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 - 管理要求：管理制度、人员管理、建设运行、应急处置	安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全建设管理、安全运维管理
	评估流程	4项：确定评估对象、开展测评工作、输出密码测评报告、密评结果上报	5项：定级、备案、建设整改、等保测评、监督检查
	评测结果	符合、部分符合、不符合	优、良、中、差

扩展补充：关基、等保和密评定义概念

01

网络安全等级测评：（简称“等保测评”）是测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动，是信息系统安全等级保护工作的重要环节。

02

关键信息基础设施安全检测评估：（简称“关基安全检测评估”）对关键信息基础设施安全性和可能存在的风险进行检测评估的活动。检测评估内容包括但不限于网络安全制度（国家和行业相关法律法规政策文件及运营者制定的制度）落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、网络安全等级保护工作落实情况、密码应用安全性评估情况、技术防护情况、云服务安全评估情况、风险评估情况、应急演练情况、攻防演练情况等，尤其关注关键信息基础设施跨系统、跨区域间的信息流动，及其关键业务流动过程中所经资产的安全防护情况。

03

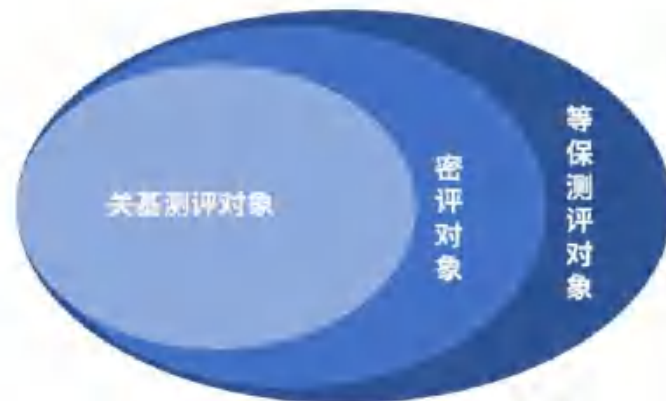
商用密码应用安全评估：（简称“密评”）是指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。

扩展补充：关基、等保和密评的评估对象联系与区别

等保测评、关基安全检测评估、密评三者的评估对象如下：

评估对象	等保测评	关基安全检测评估	密评
	1.通信网络设施 2.信息系统 ●传统信息系统 ●物联网 ●采用移动互联技术的系统 ●云计算平台/系统 ●工业控制系统 3.数据资源	关键信息基础设施：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，可能严重危害国家安全、国计民生、公共利益的信息设施。	法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施

三者评估对象关系如下：



*等级保护对象基本覆盖了全部的网络和信息系统，第三级以上的网络安全等级保护对象同时为关基和密评的评估对象，关键基础设施一定是等保测评和密评的评估对象；

密评对象是法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施等

扩展补充：关基、等保和密评的评估周期和评估内容

评估周期：等保测评、关基安全检测评估、密评在实际开展过程中应衔接进行，第三级以上的等保测评、关键基础设施、商用密码应用安全的评估周期均为每年至少一次。

评估内容：

	基本要求	评估实施指南	主要评估内容
等保测评	GB/T 22239-2019信息安全技术 网络安全等级保护基本要求	GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南	安全物理环境、安全通信网络安全区域边界、安全计算环境安全管理中心、安全管理制度安全管理机构、安全管理人员安全建设管理、安全运维管理
关基安全检测评估	信息安全技术关键信息基础设施 网络安全保护基本要求	信息安全技术 关键信息基础设施 安全检查评估指南	合规检查：关键信息基础设施认定情况、安全标准执行情况、网络安全等级保护落实情况、个人信息和重要数据保护情况、安全管理机构设置和人员安全管理情况、安全管理保证体系落实情况、备份与恢复情况、应急响应与处置情况 安全技术检测：主动监测（信息收集、漏洞扫描、漏洞验证、业务安全测试、社会工程学测试、无线安全测试、内网安全测试、安全域测试、入侵痕迹测试、安全意识测试、安全整改情况验证）、被动监测（信息探测行为监测、漏洞利用攻击监测间谍软件监测、病毒蠕虫攻击监测、木马后门攻击监测、恶意邮件攻击、Web应用攻击和漏洞监测、恶意域名监测、异常流量监测、敏感信息泄露监测） 分析评估：关键属性分析（完整性、保密性、连续性）、风险分析
密评	GB/T 39786-2021信息安全技术 信息系统密码应用基本要求	信息系统密码应用测评过程指南	通用要求、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、密码应用管理、应急响应

扩展补充：关基、等保和密评的评估流程

等级保护工作包括：

定级

备案

建设整改

等保测评

监督检查

关基网络安全保护工作包括：

识别认定

安全防护

检测评估

监测预警

事件处置

密评流程包括：

确定评估对象

开展测评工作

输出密码测评报告

密评结果上报

密评和等保测评包括

测评准备

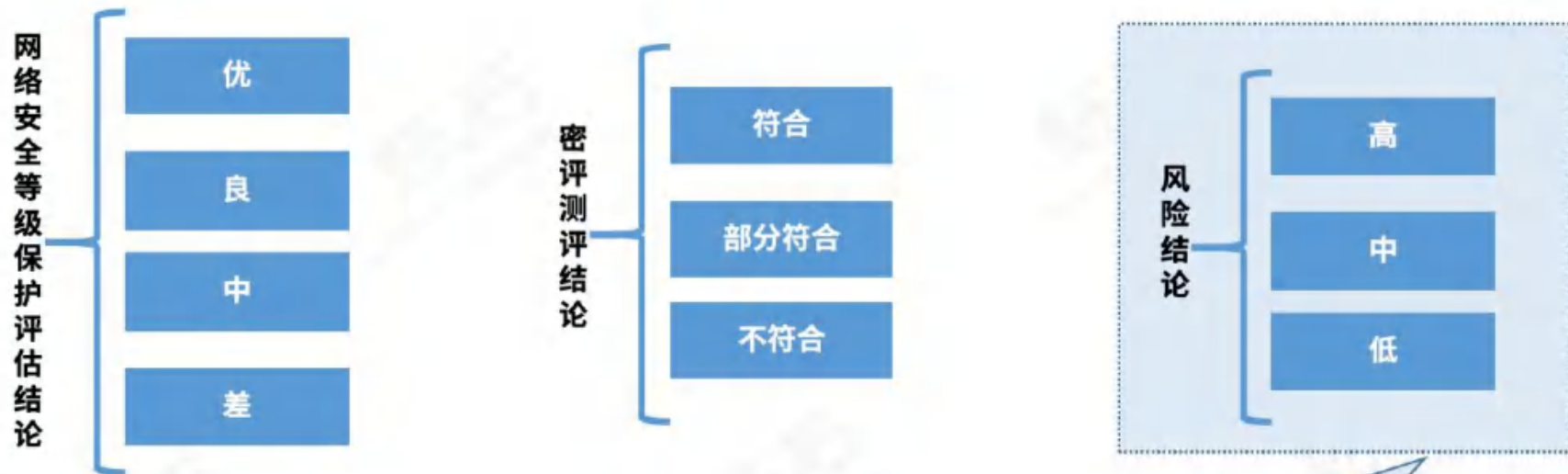
方案编制

现场测评

测评结论分析

测评报告编制

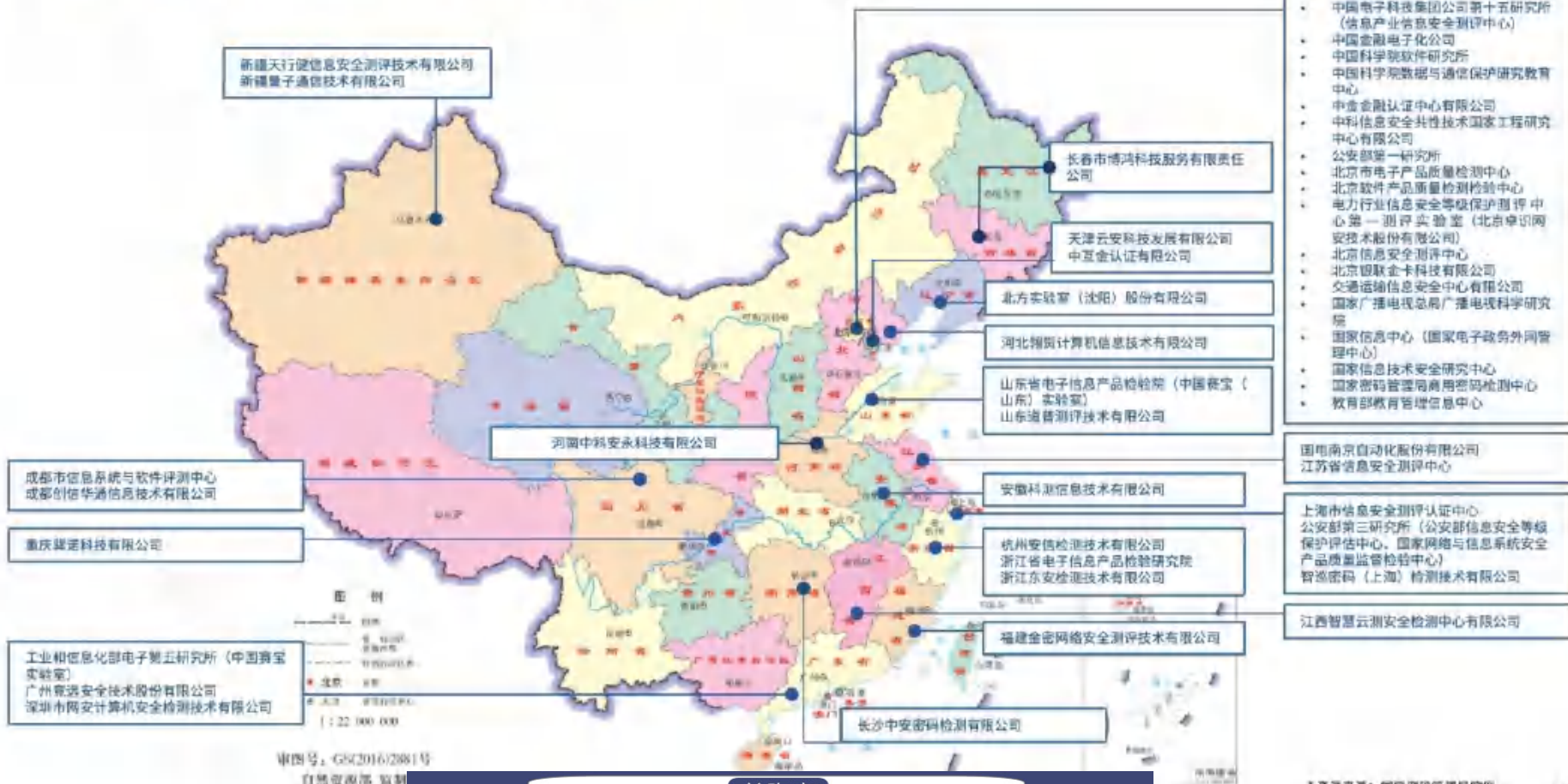
扩展补充：关基、等保和密评的评估结论



注：

- 1.关键信息基础设施保护基于风险评估的方法，重在分析安全风险可能引起的安全事件及总体安全状况。
- 2.当网络和信息系

当前已公开的48家密评机构名单一览



密评开展政策依据

发文/起草单位	发布/施行时间	政策文件	相关内容
国务院第4次常务会议审议通过	2023年4月14日	《新密码管理条例》	第三十六条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的安全和专业人员。同时规定，国家通过、同步进行商用密码保障系统，且种反攻击适用商用密码检测系统具有商用密码应用安全评估功能。 第四十一条：网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级，确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护和密码标准规范。 第四十二条：商用密码应用安全性评估、关键信息基础设施安全检测评估、网络等安全等级测评应当加强衔接，避免重复评估、测评。
公安部和网安办相关部门	2018年6月27日	《网络安全等级保护条例（征求意见稿）》	第四十七条：非涉密网络运营者应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三十七条：网络运营者采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。 第三十九条：网络运营者应当按照规划、建设和运行标准，按照密码应用安全性评估管理方法和相关标准，委托密码应用安全性评估机构开展密码应用安全性评估。网络运营者信后，方正式上线运行，并应在运行后，每年至少组织一次评估。密码应用安全性评估结果应当作为续办案件公安机关和所在地运营区的密码管理部门备案。
国务院第133次常务会议通过	2021年9月1日	《关键信息基础设施安全保护条例》	第六十条：传输、处理涉及国家秘密信息的系统信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。 关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。
国家网信办会同相关部门	2021年11月14日	《网络数据安全管理条例（征求意见稿）》	第九十条：网络运营者应当采取备份、加密、访问控制等必要措施，保障数据避免泄露、篡改、毁失、毁损、丢失、非法使用。否则就属安全事件，需按计划和对时数据的法律合规评估，维护数据的完整性、保密性、可用性。 数据运营者应当使用密码时采用密钥和核心数据进行保护。

国家层面密码应用及密评相关政策文件

发文 / 起草单位	发文时间	政策文件	相关内容
国务院	2022 年 6 月 8 日	《国务院关于加快数字政府建设的指导意见》（国发〔2022〕14 号）	第二章“构建数字政府全方位安全保障体系”第二节“落实安全制度要求”中提出：加强关键信息基础设施安全保护和网络安全等级保护，建立健全网络安全、保密监测预警和密评应用安全性评估的机制，定期开展网络安全、保密和密评应用检查，提升数字政府领域关键信息基础设施保护水平。
国务院办公厅	2022 年 1 月 20 日	《国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见》（国办发〔2022〕3 号）	第四章“全面提升电子证照应用支撑能力”第十四条“加强电子证照应用安全管理和监管”中提出：加强电子证照签发、归集、存储、使用等各环节安全管理，严格落实网络安全等级保护制度等要求，强化密评应用安全性评估，探索运用区块链、新兴密码技术、隐私计算等手段提升电子证照安全防护、追溯溯源和精准授权等能力。
国务院	2021 年 12 月 12 日	《“十四五”数字经济发展规划》（国发〔2021〕29 号）	第九章“着力强化数字经济安全体系”第一节“增强网络安全防护能力”中提出：提升网络安全应急处置能力，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力，支持开展常态化安全风险评估，加强网络安全等级保护和密评应用安全性评估。
国务院办公厅	2019 年 12 月 30 日	《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）	第三章“建设和资金管理”第十五条、第十六条中提出：项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步进行密码保障系统并定期进行评估。 项目软硬件产品的安全可信情况、项目密评应用和安全审查情况，以及硬件设备和新建数据中心能源利用效率情况是项目验收的重要内容。
国务院	2019 年 4 月 26 日	《国务院关于在线政务服务的若干规定》（国务院令 716 号）	第十三条提出：电子签名、电子印章、电子证照以及政务服务数据安全涉及电子认证、密码应用的，按照法律、行政法规和国家有关规定执行。
中共中央办公厅、国务院办公厅	2018 年 7 月 15 日	《密码应用与创新发展相关工作规划》	全面提升密码基础支撑能力，完善密码应用安全性评估审查机制。
国务院办公厅	2017 年 5 月 15 日	《政府网站发展指引》（国办发〔2017〕47 号）	第七章“安全防护”第一小节“技术防护”中提出：对重要数据、敏感数据进行分类管理，做好加密存储和传输。加强后台发布终端的安全管理，定期开展安全检查，防止终端成为后台管理系统的安全入口。使用符合国家密码管理政策和标准规范的密码算法和产品，逐步建立基于密码的网络信任、安全支撑和运行监管机制。

各部门密码应用及密评相关政策文件¹

发文/起草单位	发文时间	政策文件	相关内容
国家铁路局	2023年7月 (修)	《铁路关键信息基础设施安全保护管理办法(征求意见稿)》	第十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的铁路关键信息基础设施,运营单位应当使用商用密码进行保护,自行或者委托商用密码检测机构的每年至少开展一次商用密码应用安全性评估。 商用密码应用安全性评估应当与铁路关键信息基础设施网络安全检测和风险评估、网络安全等级测评制度相衔接,避免重复评估、测评。
国家密码管理局	2023年6月9日	《商用密码检测机构的监督管理办法(征求意见稿)》	第三条 从事商用密码产品检测、网络与信息安全商用密码应用安全性评估等商用密码检测活动,向社会出具具有证明作用的数据、结果的数据,应当经国家密码管理局认定,依法取得商用密码检测机构的资质。
国家密码管理局	2023年6月9日	《商用密码应用安全性评估管理办法(征求意见稿)》	第四条 法律、行政法规和国家有关规定要求使用商用密码进行保护的的网络与信息系統(以下统称重要网络与信息系統)。其运营者应当使用商用密码进行保护,按照商用密码应用方案,配备必要的资金和专业技术人员,开展规划、同步建设、同步运行商用密码保障系统,并定期开展商用密码应用安全性评估。
交通运输部	2023年4月24日	《公路水路关键信息基础设施安全保护管理办法》	第十八条 法律、行政法规和国家有关规定要求使用商用密码进行保护的公路水路关键信息基础设施,运营者应当使用商用密码进行保护,自行或者委托商用密码检测机构的每年至少开展一次商用密码应用安全性评估。 商用密码应用安全性评估应当与公路水路关键信息基础设施网络安全检测评估、网络安全等级测评制度相衔接,避免重复评估、测评。
国家密码管理局	2022年12月1日	《关于进一步规范商用密码应用安全性评估工作的通知》(国密局函〔2022〕434号)	进一步加强对商用密码应用安全性评估工作指导,明确重要网络与系统运营者主体责任,规范评估机构的日常监管,严格评估材料审核,包括对评估报告真实性、评估实施规范性、评估记录规范性、评估报告完整性和评估工作进行形式审查,并明确了评估机构、各级密码管理部门违规行为的处理措施。
国家铁路局	2022年11月16日	《关于印发<电力行业网络安全管理办法>的通知》(国能发安全规〔2022〕100号)	第三章“电力企业主体责任”第十五条中指出:电力企业应当按照国家有关规定开展电力监控系统安全防护评估,网络安全等级保护测评,关键信息基础设施网络安全检测和风险评估,商用密码应用安全性评估和网络信息安全审查等工作,及时整改隐患及发现的问题。
国家卫生健康委员会、国家中医药局、国家疾控局	2022年8月3日	《医疗卫生机构网络安全管理办法》(国卫规划发〔2022〕29号)	第二章“网络安全管理”第十五条中指出:各医疗卫生机构应按照国家有关规定开展网络安全等级保护测评,网络安全等级保护测评,商用密码应用安全性评估和网络信息安全审查等工作,及时整改隐患及发现的问题。

发文/起草单位	发文时间	政策文件	相关内容
国家能源局、国家发展改革委、交通运输部	2021年12月28日	《“十四五”能源电力发展规划》	第二步“重点任务”第六条“提升网络安全水平”中第十九条提出:加强网络安全防护,严格落实网络安全等级保护制度,完善行业网络安全,加强安全风险评估,在网络安全等级保护中,同步规划、建设、使用有关安全防护措施,严格落实国家关于等级保护、网络安全等要求,加强行业关键信息基础设施保护,加强网络安全规划,落实行业指导和监管,加强行业网络安全和个人信息保护。
民航局	2021年12月23日	《关于印发<“十四五”民航信息化建设规划>的通知》(民航〔2021〕104号)	第三章“重点任务”第四十条提出:全面开展民用航空网络安全,构建覆盖统一的网络安全基础服务平台,提供统一的数据传输、存储和身份认证管理等基础服务,提升密码应用和管理水平。
国家密码管理局	2021年11月26日	《关于规范商用密码应用安全性评估实施工作的通知》(国密局〔2021〕321号)	网络与信息安全业务同步规划、同步建设、同步运行商用密码保障系统,规范评估工作,履行备案程序。密码管理机构对评估机构评估材料进行审核,定期开展汇总备案抽查,指导督促商用密码应用安全性评估工作,评估机构统计评估工作评估数据报送密码管理局。
国家密码管理局、中央网信办、国家发展和改革委员会、科技部、工业和信息化部、公安部、财政部、国务院国资委、银保监会、证监会	2021年11月20日	《促进商用密码产业高质量发展实施意见》	依法督促通过密码检测评估,并开展重要网络与信息安全商用密码应用安全性评估的执法检查。
工业和信息化部	2021年9月15日	《关于加强工业互联网网络安全保障工作的通知》(工信部函〔2021〕114号)	第四章“加强工业互联网网络安全保障”第十六条中指出:认定为关键信息基础设施的,应当落实《关键信息基础设施网络安全保护条例》有关规定,开展国家网络安全审查并按照国家规定进行保护,自行或者委托商用密码检测机构的商用密码应用安全性评估。
工业和信息化部、中央网信办、科技部、工业和信息化部、公安部、财政部、国务院国资委、银保监会、证监会	2021年9月10日	《物联网新型基础设施建设三年行动计划(2021-2023年)》(工信部科〔2021〕110号)	第二步“重点任务”第六条“提升网络安全保障”中第十二条提出:加强物联网网络安全保障技术和产品的应用推广,建议由物联网领域密码应用检测平台,提升物联网领域商用密码应用安全性和应用水平。

各部门密码应用及密评相关政策文件²

发文/起草单位	发文时间	政策文件	相关内容
工业和信息化部、中央网信办、国家发展和改革委员会、教育部、财政部、住房和城乡建设部、工业和信息化部、国家卫生健康委员会、国家知识产权局	2021年10月5日	《5G应用“扬帆”行动计划(2021-2023年)》(工信部规〔2021〕77号)	第十四条“提升5G应用水平”第三点“5G应用融合提升行动”中第二点指出,在5G应用中推广使用密码,提升密码应用水平。
交通运输部办公厅	2021年11月27日	《交通运输部“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第九章“互联网业务”第四点“运营安全”中第九点指出,交通运输部将加强密码应用和管理,推动密码应用安全使用,提升密码应用水平。
住房和城乡建设部、中央网信办、国家发展和改革委员会、教育部、工业和信息化部、国家卫生健康委员会、国家知识产权局	2021年4月6日	《住房和城乡建设部“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第十四条“互联网业务”第四点“运营安全”中第九点指出,住房和城乡建设部将加强密码应用和管理,推动密码应用安全使用,提升密码应用水平。
国家卫生健康委员会	2020年9月27日	《国家卫生健康委员会“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第二章“网络安全”第四点“运营安全”中第九点指出,国家卫生健康委员会将加强密码应用和管理,推动密码应用安全使用,提升密码应用水平。

发文/起草单位	发文时间	政策文件	相关内容
公安部	2020年7月22日	《公安机关人民警察使用网络应用程序管理规定》(公安部令〔2020〕第100号)	第二章“深入贯彻执行国家网络安全等级保护制度”第六点中指出,公安机关人民警察使用网络应用程序,应当符合网络安全等级保护制度要求,并符合网络安全等级保护制度要求。
国家发展改革委办公厅	2020年7月9日	《关于加快推进“互联网+政务服务”工作的指导意见》(发改办〔2020〕122号)	第二章“重点任务”第四点中指出,推进“互联网+政务服务”工作,应当符合网络安全等级保护制度要求,并符合网络安全等级保护制度要求。
教育部办公厅	2020年2月26日	《教育部“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第三章“网络安全”第五点“网络安全能力建设”中指出,教育部将加强网络安全能力建设,提升网络安全保障能力。
水利部办公厅	2020年2月14日	《水利部“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第一章“总体要求”第一条“总体要求”中指出,水利部将加强网络安全和信息化建设,提升网络安全保障能力。
交通运输部	2019年12月10日	《交通运输部“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第二章“重点任务”第四点“网络安全能力建设”中指出,交通运输部将加强网络安全能力建设,提升网络安全保障能力。
国家能源局	2018年9月23日	《国家能源局“十四五”网络安全和信息化发展规划(2021-2025年)》(交办函〔2021〕27号)	第三章“网络安全”第五点“网络安全能力建设”中指出,国家能源局将加强网络安全能力建设,提升网络安全保障能力。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	主要内容
	2020年11月	《关于进一步加强非涉密信息系统运营管理与网络安全评估工作的通知》(冀网安局字〔2020〕12号)	落实《河北省政务信息系统运营项目建设管理办法》(冀政办字〔2020〕48号)要求,规范省内非涉密政务信息系统运行、运维、验收阶段保密保障体系建设、管理,落实“同步、同步评”要求。
河北省	2020年4月	《河北省政务信息系统运营项目建设管理办法》(冀政办字〔2020〕48号)	第十九条提出:项目建设单位应当落实国家网络安全管理法律法规,按照标准规范建设,同步建设、同步验收、同步进行网络安全等级保护定级测评工作。
	2019年3月	《关于开展重要信息系统密码应用安全性评估的通知》(冀网安局字〔2019〕2号)	望切实加强密文传输,组织开展省内重要针对县建设使用的重要信息系统密码应用安全性评估。省密码管理部门的工作情况和评估发现问题开展监督检查。
	2022年10月	《山西省财政厅关于在政府采购中落实密码应用的通知》(晋财〔2022〕13号)	落细落实机关严格依照《密码法》及相关要求落实密码应用,涉及密码及密码相关的信息化项目采购合同中同步建设、同步进行密码保障建设,保障网络和信息安全。
山西省	2021年8月	《山西省政务云管理办法》(晋政办发〔2021〕72号)	第五章“安全管理”第二十四条中指出:政务云数据提供方和政务云使用方应当严格落实密码应用法律法规和相关政策,使用符合国家技术标准和规范的信息产品及其管理,优先使用自主可控的软硬件产品,定期开展密码应用安全评估。
	2019年9月	《山西省政务云项目运营后管理暂行办法》(晋政办发〔2019〕72号)	第五章“管理和安全”第三十七条中指出:项目实施单位与项目建设单位共同开展网络与信息安全风险评估,严格落实密码保护和密码应用管理要求,同步建设、同步进行密码保障体系建设并测评评估,切实保障政务信息系统核心安全稳定运行。
内蒙古自治区	2023年1月	《内蒙古自治区“十四五”期间政务网络重点工程任务》(内网安局发〔2023〕1号)	如加强密码应用应用安全保障和管理,推动关键信息基础设施,等级保护三级及以上信息系统,全自治区信息系统等同步规划、同步建设、同步落实密码保障建设,完善网络安全和密码应用安全保障体系;加强与政务云信息化管理部门的工作协同,严格落实密码应用保障管理要求,加强对密码机构的指导和督促;探索建立用户评价机制,持续提升密码机构的服务水平;推动国家信息资源、数据科学布局、数据应用、密码技术创新等,加快推进密码应用基础设施应用安全性能提升,持续优化“内蒙古自治区政务网络网络安全保障工程”建设,推进重要密码应用试点应用,加强

各省(自治区、直辖市)及新疆生产建设兵团密码应用及密评政策²

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
内蒙古自治区	2022年12月	《自治区系统信息安全项目建设管理办法》(内发改政投字〔2022〕1963号)	第十二条第二款规定:系统信息安全包括项目立项、实施、验收应用安全审查和密码应用安全评估评估内容。
	2022年11月	《内蒙古自治区数字政务建设条例》(第41号)	第三十条规定:各级政府和建设(代建)单位应当严格落实网络安全等级保护制度规定,新建系统、升级改造系统应当符合网络安全等级保护要求,并定期开展网络安全风险评估和等级测评,将政务信息系统运行安全纳入政务信息安全管理考核体系。
	2022年1月	《关于规范自治区密码应用安全评估工作的通知》(内密局发〔2022〕1号)	第六条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。
	2021年11月	《关于规范自治区系统信息安全项目建设的通知》(内密局发〔2021〕7号)	一、各级新建系统信息安全项目应当符合国家密码管理应用安全法律法规和标准规范要求,同步规划、同步建设、同步运行密码保障体系,开展定期评估。
	2021年9月	《内蒙古自治区密码应用安全评估办法》(内密局发〔2021〕5号)	第三条“适用范围”第七条“组织管理”规定:密码应用安全评估工作由自治区密码管理局负责,各盟市、旗县区密码管理部门负责实施。
辽宁省	2021年6月	《辽宁省系统信息安全项目建设的通知》(辽发改投〔2021〕183号)	第十二条“中密所密”第七条“工程建设项目”规定:工程建设项目应当符合密码应用安全评估要求,并符合项目建设和使用要求。项目建设单位应当严格落实密码应用安全评估要求,并定期开展网络安全风险评估和等级测评。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
辽宁省	2021年10月	《关于进一步规范和加强系统信息安全项目建设的通知》(辽密局发〔2021〕26号)	第三条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。
	2022年5月	《关于规范和加强系统信息安全项目建设的通知》(辽密局发〔2022〕1号)	第六条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。
	2021年12月	《关于规范和加强系统信息安全项目建设的通知》(辽密局发〔2021〕21号)	第六条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。
	2021年5月	《关于规范和加强系统信息安全项目建设的通知》(辽密局发〔2021〕18号)	第六条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。
新疆维吾尔自治区	2021年10月	《关于进一步规范和加强系统信息安全项目建设的通知》(新密局发〔2021〕26号)	第三条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。
	2021年5月	《关于规范和加强系统信息安全项目建设的通知》(新密局发〔2021〕18号)	第六条“基本原则”第十四条规定:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和应急响应,网络安全等级保护、密码应用安全评估、数据安全风险评估等安全技术措施,保障数据、网络、设备等方面的安全。

各省(自治区、直辖市)及新疆生产建设兵团密码应用及密评政策³

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
黑龙江省	2022年1月	《关于规范商用密码应用安全性评估工作通知》	黑龙江省和黑龙江省公安厅等相关部门，开展商用密码应用安全性评估工作，同时建设、同时使用商用密码应用系统，自行或委托具有商用密码应用安全性评估资质，履行备案程序。自评估报告出具之日起30日内，填写《商用密码应用安全性评估备案表》，报同级密码管理部门备案。
	2021年12月	《黑龙江省“十四五”政务信息化建设规划》(黑政发〔2021〕17号)	第四章“夯实网络安全基础”第四章“构建全省一体化安全防护体系”第一节“提升全省网络安全能力”中提出：完善密码基础设施，健全密码服务体系，全面提升密码应用和可信信息支撑，强化密码保护技术支撑能力，加强密码应用基础设施服务能力，同步规划、同步建设、同步运行密码保障系统，推进政务信息基础设施密码应用，开展密码应用评估。
	2021年4月	《黑龙江省密码应用管理办法》(黑政办发〔2021〕17号)	第一章“总则”第六十条规定：国家机关依照国家密码管理法律法规和标准规范从事密码应用、同步规划、同步建设、同步运行密码保障系统。
	2020年11月	《关于进一步加强政务信息基础设施密码应用与安全性评估工作的通知》	黑龙江省和黑龙江省公安厅等相关部门依照国家密码管理法律法规和标准规范从事密码应用、同步规划、同步建设、同步运行密码保障系统。
上海市	2022年8月	《上海市密码应用项目立项管理暂行办法》(沪府规〔2022〕33号)	明确商用密码产品、密码服务列入建设清单，密码应用项目立项审批，密码应用项目立项审批意见之一，项目立项审批意见要求，项目立项审批意见及密码应用项目审批意见。
	2022年5月	《上海市重要网络和信息系统密码应用与安全性评估工作指南(2022版)》	第二章“密码应用与安全性评估范围”中规定：对于涉及国家安全和公共利益的重要网络和信息系统，包括从事经营活动的重要基础设施、网络安全等级保护第三级以上网络(含信息系统)、政务信息系统、研发设计、行政决策和重要业务系统、涉及使用商用密码保护的系统和信息系统，应当落实密码应用法律法规、管理办法和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。
	2022年4月	《上海市重要网络和信息系统密码应用与安全性评估工作指南(2022版)》	第三章“密码应用与安全性评估范围”中规定：对于涉及国家安全和公共利益的重要网络和信息系统，包括从事经营活动的重要基础设施、网络安全等级保护第三级以上网络(含信息系统)、政务信息系统、研发设计、行政决策和重要业务系统、涉及使用商用密码保护的系统和信息系统，应当落实密码应用法律法规、管理办法和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。
	2022年4月	《上海市政务云管理办法》(沪府办〔2022〕8号)	政务云主管部门、政务云的运营管理机构和使用单位应当严格落实国家网络安全和密码应用法律法规，采取安全措施，并与政务云运营机构、运营建设、运营维护网络安全责任密码保障体系。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
上海市	2022年4月	《上海市电子政务基础设施密码应用与安全性评估工作指南(2022版)》	可用于指导政务部门办公信息系统的责任单位开展密码应用与安全性评估工作，也可作为相关标准、规范的支撑和补充。密码应用与安全性评估工作，应当参照《上海市电子政务基础设施密码应用与安全性评估工作指南(2022版)》开展相关工作。
	2022年2月	《关于进一步加强上海市电子政务基础设施密码应用与安全性评估工作的通知》	加强上海市电子政务基础设施密码应用与安全性评估工作。
	2021年5月	《关于规范和加强上海市重要网络和信息系统密码应用与安全性评估工作的通知》(含上海市重要网络和信息系统密码应用与安全性评估工作指南(2021版))	明确密码应用与安全性评估的范围、要求、工作实施流程和保护措施。规范和加强上海市重要网络和信息系统密码应用与安全性评估工作。
	2020年3月	《关于进一步加强和规范上海市重要网络和信息系统密码应用工作的通知》	规范和加强上海市重要网络和信息系统密码应用与安全性评估工作。
江苏省	2022年4月	《省政府关于加快推进数字政府建设促进数字经济高质量发展的实施意见》(苏政发〔2022〕44号)	第五章“织密网络安全数据安全防护网”第十六条“严格执行安全管理规定”中提出：依法加强数据安全保护，落实网络安全等级保护、关键信息基础设施安全防护、数据安全分级保护、密码应用管理标准。
	2022年3月	《关于规范和加强江苏省重要网络和信息系统密码应用与安全性评估工作的通知》(苏府规〔2022〕7号)	进一步规范各有关部门、单位密码应用与备案工作，明确密码应用与备案工作情况作为网络安全工作考核的重要内容，有关密码管理考核。
	2021年4月	《江苏省重要网络和信息系统密码应用与安全性评估工作指南(2021版)》(苏政办发〔2021〕24号)	第二章“建设和安全管理”第十六条中提出：项目建设单位应当落实国家和省密码管理法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。
	2020年8月	《江苏省政务信息资源目录管理办法》(试行)(苏政办发〔2020〕43号)	随文提出政务信息资源目录密码应用与评估备案工作的要求和工作流程。

地区/行政区、直辖市、新疆生产建设兵团	发布时间	政策文件	涉及领域
安徽省	2021年1月	《数字安徽建设2021年重点工作安排》	加强基础设施、数据中心、工业互联网平台等基础设施建设和保护及支付、不断开展网络安全保护和利用网络新技术等任务。
	2022年11月	《安徽省政务服务信息化项目建设管理办法》（皖政办〔2022〕2号）	第四章“项目建设管理”第三十条中指出：项目建设单位应按照国家密码管理局《密码使用规范和标准规范指南》、《密码法》、《网络安全法》、《网络安全等级保护基本要求》等法律法规和国家标准，对涉及密码应用系统实施密码应用安全性评估。
	2022年度	《安徽省电子政务密码应用安全评估考核办法》	《安徽省电子政务密码应用安全评估考核办法》于2022年11月1日起实施，旨在规范电子政务密码应用安全评估工作，提升电子政务密码应用安全水平。该办法明确了评估范围、评估内容、评估程序、评估结果应用等方面的工作要求。
	2021年12月	《关于推进密码应用与网络安全等级保护深度融合的通知》	该通知要求，各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。
	2022年12月	《安徽省电子政务密码应用安全评估考核办法》（皖政办〔2022〕43号）	该办法旨在规范电子政务密码应用安全评估工作，提升电子政务密码应用安全水平。该办法明确了评估范围、评估内容、评估程序、评估结果应用等方面的工作要求。
福建省	2022年12月	《福建省电子政务密码应用安全评估考核办法》（闽政办〔2022〕43号）	该办法旨在规范电子政务密码应用安全评估工作，提升电子政务密码应用安全水平。该办法明确了评估范围、评估内容、评估程序、评估结果应用等方面的工作要求。
	2022年1月	《关于推进密码应用与网络安全等级保护深度融合的通知》	该通知要求，各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。
	2021年11月	《福建省“十四五”电子政务密码应用安全规划》（闽政办〔2021〕25号）	第八章“密码应用与网络安全等级保护深度融合”第二十条中指出：各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。
	2017年11月	《关于推进密码应用与网络安全等级保护深度融合的通知》	该通知要求，各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。
江西省	2021年11月	《江西省电子政务密码应用安全评估考核办法》（赣政办〔2021〕63号）	第六章“安全评估”第二十条中指出：各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。
	2021年11月	《江西省电子政务密码应用安全评估考核办法》（赣政办〔2021〕63号）	第六章“安全评估”第二十条中指出：各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。
	2020年9月	《江西省电子政务密码应用安全评估考核办法》（赣政办〔2020〕68号）	第六章“安全评估”第二十条中指出：各级党政机关、企事业单位、社会团体等应积极推进密码应用与网络安全等级保护的深度融合，确保密码应用与网络安全等级保护的同步规划、同步建设、同步实施、同步评估、同步整改。

国(区)酒店、 图书馆、 博物馆生产建 筑项目	发布时间	法规文件	规范内容
	2022年10月	《河南省加强公共安全设施“四电”扩大应用和互通互认实施办法》(豫政发〔2022〕101号)	提高“四电”支撑能力。创新安全技术保障模式，严格落实网络信息安全保护。落实国家网络安全等级保护要求，增强自主可控水平。
	2022年9月	《河南省大数据产业发展和应用促进(2022-2025年)》(豫政发〔2022〕80号)	第三条“主要任务”第三节“构建安全治理体系”中提出：实施网络安全“铸盾”工程，完善网络安全技术和标准安全防护。风险评估、漏洞扫描等安全态势感知。依法使用网络安全数据资源，完善网络安全事件评估；建立网络安全等级保护和数据安全审查制度。
	2022年4月	《河南省政务数据共享管理暂行办法》(豫政办〔2022〕10号)	第七条提出：网信部门负责统筹协调、指导监督和有关监督管理工作。公安网安负责等级保护、可信认证、涉法监督、信息通报、应急处置等监督管理工作。保密、国家安全、应急管理、大数据管理、通信管理等相关部门配合开展有关工作。法院、检察院、公安机关、商务等部门按照职责承担相关监管职责。
河南高院	2022年1月	《河南省“十四五”新型基础设施规划》(发改能源〔2022〕32号)	“第四十二条基础网络全面提升关键信息基础设施防护范围，提升国家安全防护能力。强化新型基础设施监测，同步建设、同步使用。”“健全网络安全应急响应机制，构建攻防兼备的安全技术支撑体系，提升重要基础设施安全保障能力。”“提升安全可信。全面实行网络安全产品和服务认证，深化密码技术应用，提升重要基础设施应用可信。”“严格落实网络安全主体责任，严格执行网络安全等级保护、商用密码应用安全性评估等相关法规和标准规范要求。”
	2021年12月	《关于组织开展商用密码应用安全性评估和风险备案工作的通知》(豫密局发〔2021〕33号)	依据《关于组织开展商用密码应用安全性评估和风险备案工作的通知》(国密厅字〔2021〕102号)。河南省委区域网信办部署相关工作进行部署安排，派出有关负责同志。
	2021年10月	《关于省电力业务系统电网网络和综合系统内网应用安全等级保护工作的通知》(信安函电〔2021〕40号)	2021年10月，河南省密管办向国网河南省电力公司印发，要求各单位对已建成业务系统网络和信息设备开展商用密码应用安全性检查，并加贴标识规范运行维护。
	2021年11月	《关于进一步加快推进政务社会事务类商用密码应用与安全管理等级保护工作的通知》(豫密局发〔2021〕66号)	依据国家密码管理局《关于加快推进政务社会事务类商用密码应用与安全管理等级保护工作的通知》(国密局公〔2020〕119号)，河南省密管办、发展改革委、网信办、无线电管理局联合发文。就河南省加快推进政务社会事务类商用密码应用与安全管理等级保护工作进行“四早一升级”。根据商用密码应用与安全性评估结果，把商用密码等级保护和等级保护要求统一。

省(自治区、直辖市)、 新疆生产建设兵团	发布时间	政策文件	相关内容
湖北省	2015年12月	《关于推进电子政务协同发展的指导意见》(鄂政发〔2015〕93号)	完善安全防护体系。加强密码应用规范的落实,构建基于电子政务安全防护体系。制定统一安全策略,制定安全策略、部署策略和应急响应,重要信息资源库、业务系统等和重要信息资源的应用,根据信息资源部署建设,建立动态安全检查和评估规范的统一性、数据管理、可信时间安全策略实施,加大自主可控安全产品应用,强化安全保密管理,加强日常安全管理,完善密码管理相关主体责任。
湖南省	2022年3月	《湖南省电子政务网络安全审查规范》(DB43/T 2133-2022)	第五章“安全审计规范”第一节“审计编制”中指出,建设国家关键信息需求应用安全审计,并按照国家网络安全等级保护安全审计要求,安全审计方案包含密码安全审计设备审计方案,按照国家方案,按照安全保护方案。
	2020年8月	《湖南省电子政务信息安全应用系统安全管理规范》(湘规办发〔2020〕34号)	第三章“系统安全和安全”第六节六条中指出,项目建成后,应按照国家密码管理有关法律法规和标准规范,同步建设、同步使用、同步运行,同步进行安全评估和认证,并按照国家密码应用安全评估和认证不合格的,不得进行推广应用,不得投入使用。
广东省	2023年2月	《广东省电子政务系统信息安全等级保护实施指南》(粤网安办〔2023〕2号)	广东省密码管理局与16个部门联合发布行政计划,进一步保障“信息安全等级保护实施指南”实施,同时建设同步进行密码应用系统,完善国家密码应用安全评估和认证,并按照国家密码应用安全评估和认证“安全”等要求。
	2022年12月	《广东省电子政务系统信息安全等级保护实施指南》(粤网安办〔2022〕11号)	按照国家密码管理局有关文件精神,结合《广东省电子政务系统信息安全等级保护实施指南》,广东省密码管理局印发通知。
	2021年12月	《广东省电子政务系统信息安全等级保护实施指南》(粤网安办〔2021〕7号)	按照国家密码管理局有关文件精神,结合《广东省电子政务系统信息安全等级保护实施指南》,广东省密码管理局印发通知。
	2021年3月	《广东省电子政务系统信息安全等级保护实施指南》(粤网安办〔2021〕3号)	在粤网安办〔2021〕9号文件基础上,进一步明确涉及国家电子政务系统信息安全等级保护实施指南的要求和标准。
	2020年6月	《广东省电子政务系统信息安全等级保护实施指南》(粤网安办〔2020〕12号)	在粤网安办〔2021〕9号文件基础上,进一步明确涉及国家电子政务系统信息安全等级保护实施指南的要求和标准。

各省(自治区、直辖市)及新疆生产建设兵团密码应用及密评政策⁷

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
广东省	2020年6月	《广东省政务密码应用管理办法(征求意见稿)》(广东省政务信息基础设施项目验收符合性检测指南)《通知》(粤政办〔2020〕13号)	密码应用(2020)9号:在此基础上,进一步明确密码应用对系统运行管理、数据安全、业务连续性等要求。
	2020年6月	《广东省政务信息基础设施项目验收符合性检测指南》(粤政办〔2020〕13号)	密码应用(2020)9号:在此基础上,进一步明确密码应用对系统运行管理、数据安全、业务连续性等要求。
	2020年4月	《广东省人民政府办公厅关于印发广东省政务信息基础设施项目验收符合性检测指南》(粤政办〔2020〕9号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
广西壮族自治区	2022年9月	《关于加快推进数字化转型发展融入粤港澳大湾区建设的实施意见》(桂发〔2022〕18号)	第一章“总体要求”第二条中指出:“加快推进数字化转型,提升发展质量和安全水平。坚持创新驱动,提升发展质量和安全水平。坚持创新驱动,提升发展质量和安全水平。”
	2021年12月	《广西壮族自治区“十四五”规划纲要》(桂发〔2021〕18号)	“加快推进数字化转型,提升发展质量和安全水平。坚持创新驱动,提升发展质量和安全水平。”
	2021年3月	《广西壮族自治区“十四五”规划纲要》(桂发〔2021〕18号)	“加快推进数字化转型,提升发展质量和安全水平。坚持创新驱动,提升发展质量和安全水平。”
海南省	2022年11月	《海南省政务信息基础设施项目验收符合性检测指南》(琼发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
海南省	2022年9月	《海南省政务信息基础设施项目验收符合性检测指南》(琼发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
	2022年7月	《海南省政务信息基础设施项目验收符合性检测指南》(琼发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
	2022年7月	《海南省政务信息基础设施项目验收符合性检测指南》(琼发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
	2022年6月	《海南省政务信息基础设施项目验收符合性检测指南》(琼发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
	2021年7月	《海南省政务信息基础设施项目验收符合性检测指南》(琼发〔2021〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
重庆市	2022年7月	《重庆市政务信息基础设施项目验收符合性检测指南》(渝发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”
	2022年7月	《重庆市政务信息基础设施项目验收符合性检测指南》(渝发〔2022〕10号)	“密码应用应符合项目业务需求,按照密码应用安全标准,对密码应用的安全需求进行安全评估。”

各省(自治区、直辖市)及新疆生产建设兵团密码应用及密评政策⁸

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
重庆市	2021年11月	《重庆市市民信息保护管理办法》(市政府令〔2021〕122号)	第四章“监督管理”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2021年2月	《关于切实加强重要信息安全管理的通知》(重信安〔2021〕10号)	第九条指出:市政务服务中心应当严格落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
四川省	2021年2月	《关于进一步加强重要信息安全管理的通知》(川信安〔2021〕10号)	第九条指出:市政务服务中心应当严格落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2022年10月	《四川省政务信息安全管理规定》(省政府令〔2022〕118号)	第四章“监督管理”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2022年4月	《四川省政务信息安全管理规定》(省政府令〔2022〕118号)	第四章“监督管理”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2022年4月	《四川省政务信息安全管理规定》(省政府令〔2022〕118号)	第四章“监督管理”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2022年4月	《四川省政务信息安全管理规定》(省政府令〔2022〕118号)	第四章“监督管理”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
四川省	2021年4月	《四川省“十四五”政务信息安全管理规划》(川信安〔2021〕24号)	第四章“安全保障”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2021年4月	《四川省“十四五”政务信息安全管理规划》(川信安〔2021〕24号)	第四章“安全保障”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
贵州省	2021年3月	《关于进一步加强重要信息安全管理的通知》(贵信安〔2021〕10号)	第九条指出:市政务服务中心应当严格落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2021年3月	《关于进一步加强重要信息安全管理的通知》(贵信安〔2021〕10号)	第九条指出:市政务服务中心应当严格落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
云南省	2021年4月	《云南省“十四五”政务信息安全管理规划》(云信安〔2021〕24号)	第四章“安全保障”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。
	2021年4月	《云南省“十四五”政务信息安全管理规划》(云信安〔2021〕24号)	第四章“安全保障”第六十五条中指出:市政务服务中心应当严格落实国家信息安全法律法规,建立健全信息安全管理规章制度,落实信息安全责任制,落实信息安全风险评估、安全等级保护、安全审计、安全监测、安全预警、安全应急处置等制度,确保信息安全。

各省(自治区、直辖市)及新疆生产建设兵团密码应用及密评政策⁹

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
西藏自治区	2022年7月	《西藏自治区密码应用安全风险评估工作指南(试行)》(藏密局发〔2022〕3号)	结合应用需求和西藏自治区密码应用安全风险评估指南,明确西藏自治区密码应用安全风险评估工作指南,指导西藏自治区密码应用安全风险评估工作,提高西藏自治区密码应用安全风险评估工作水平。
	2022年4月	《西藏自治区电子政务密码应用安全管理规定》(藏政办发〔2022〕14号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年12月	《关于规范西藏自治区网络安全风险评估工作的通知》(藏密局发〔2021〕4号)	该办法规定西藏自治区网络安全风险评估工作的具体要求:
陕西省	2023年2月	《关于陕西省电子政务密码应用安全管理规定》(陕政办发〔2023〕2号)	第四条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2022年4月	《陕西省电子政务密码应用安全管理规定》(陕政办发〔2022〕14号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2022年6月	《陕西省电子政务密码应用安全管理规定》(陕政办发〔2022〕14号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年10月	《陕西省电子政务密码应用安全管理规定》(陕政办发〔2021〕10号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年10月	《陕西省电子政务密码应用安全管理规定》(陕政办发〔2021〕10号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
甘肃省	2022年4月	《甘肃省电子政务密码应用安全管理规定》(甘政办发〔2022〕50号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年12月	《甘肃省电子政务密码应用安全管理规定》(甘政办发〔2021〕113号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年12月	《甘肃省电子政务密码应用安全管理规定》(甘政办发〔2021〕113号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年12月	《甘肃省电子政务密码应用安全管理规定》(甘政办发〔2021〕113号)	第二条“建设和安全管理”章节中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
青海省	2020年5月	《关于青海省电子政务密码应用安全管理规定》(青政办发〔2020〕38号)	第二条“建设和安全管理”第十八条中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2020年5月	《关于青海省电子政务密码应用安全管理规定》(青政办发〔2020〕38号)	第四条“建设和安全管理”第三十二条中规定:各部门应严格落实密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
宁夏回族自治区	2021年1月	《关于宁夏回族自治区电子政务密码应用安全管理规定》(宁政办发〔2021〕1号)	第二条“建设和安全管理”第十八条中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年1月	《关于宁夏回族自治区电子政务密码应用安全管理规定》(宁政办发〔2021〕1号)	第四条“建设和安全管理”第三十二条中规定:各部门应严格落实密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
新疆维吾尔自治区	2021年12月	《新疆维吾尔自治区电子政务密码应用安全管理规定》(新政办发〔2021〕113号)	第二条“建设和安全管理”第十八条中规定:项目建设和运营各方应严格按照密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。
	2021年12月	《新疆维吾尔自治区电子政务密码应用安全管理规定》(新政办发〔2021〕113号)	第四条“建设和安全管理”第三十二条中规定:各部门应严格落实密码应用安全标准规范的要求,同步规划、同步建设、同步运行密码应用系统并定期进行评估。

各省(自治区、直辖市)及新疆生产建设兵团密码应用及密评政策¹⁰

省(自治区、直辖市)、新疆生产建设兵团简称	发布时间	政策文件	相关内容
宁夏回族自治区	2021年6月	《宁夏回族自治区贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的实施意见》(宁公[网安]通[2021]42号)	网络运营者要按照国家网络安全《中华人民共和国密码法》等法律法规规定和密码应用相关标准规范,新建第三级(含)以上网络,运营者要按照“三同步”的要求,同步采取密码技术对网络系统进行保护,并使用符合相关法律法规规定的密码产品和服务。已运行的第三级(含)以上网络运营者要在网络规划、建设阶段同步规划密码安全防护措施,在网络安全等级测评中同步开展密码应用安全评估,正式运行后,每年至少评估一次。评估完成后,应在30个工作日内将评估结果报所在地密码管理部门、公安部门备案。
新疆维吾尔自治区	2023年2月	《新疆维吾尔自治区密码管理局关于进一步规范自治区商用密码应用建设和安全评估工作的通知》(新机发[2023]1号)	第二章“规范开展密码应用安全性评估”中提出:“明确范围。网络安全等级保护三級以上网络和信息系统应开展商用密码应用安全性评估。其中金融、能源、交通、水利、电子政务(如门户网站等)系统应开展评估;其他系统按照接入上级部门建设的业务信息系统的,或具备本地接入用户,系统运维管理责任明确,或在本地进行数据汇聚、系统集中部署等实际情况,开展评估。”“明确流程。各地各部门应积极配合承担各负责的第二方测评机构开展商用密码应用安全性评估,不得委托信息系统集成商全权代理,不得干扰第三方测评机构独立开展工作,不得影响于评估结果。”
	2023年2月	《新疆维吾尔自治区公共数据管理办法(试行)》(新政办发[2023]11号)	第七章“监督管理”第三十八条中提出:公共数据提供部门、公共数据使用部门,应当建设数据管理部门建设“数据源、数据流、数据用、数据管、数据保、数据查”的架构,按照国家信息安全等级保护、数据安全分级管理、密码应用安全保护要求,在公共数据管理全流程过程中加强安全防护、访问控制、权限管理、全流程审计等网络安全管理和防护。
	2021年2月	《新疆维吾尔自治区密码管理局关于深入贯彻商用密码法进一步健全完善商用密码应用和安全评估工作的指导意见》(新密函[2021]14号)	第二章“健全完善密码应用工作准备机制”中提出:“责任单位要落实密码应用管理工作纳入项目建设各环节。规划阶段:新建单位应依据密码应用有关规定,制定商用密码应用建设方案,组织专家或委托测评机构进行风险评估,论证和签署必要条件列入项目立项材料并报送密码管理部门备案。建设阶段:责任单位应委托第三方测评机构进行商用密码应用安全评估,评估通过后方可项目验收和投入运行。运维阶段:责任单位应定期开展商用密码应用安全评估,评估报告报送密码管理部门备案。”

省(自治区、直辖市)、新疆生产建设兵团简称	发布时间	政策文件	相关内容
新疆维吾尔自治区	2021年2月	《新疆维吾尔自治区政务信息化项目建设管理办法》(新政办发[2021]14号)	第十四条提出:项目建设单位应当落实《中华人民共和国密码法》,自治区密码管理局有关法规规章和标准规范要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。
新疆生产建设兵团	2021年12月	《兵团办公厅关于印发《兵团政务信息化项目建设管理办法(试行)》的通知》(新兵团办[2021]126号)	第七章“安全管理”第四十七条中提出:项目建设单位落实国家网络安全、数据安全、个人信息保护、密码管理有关法律法规和标准规范的要求,建立网络安全、数据安全制度,加强政务信息系统与信息资源系统的安全建设、建设、同步规划、同步建设、同步运行网络安全、密码保障系统并定期进行检测和评估。

更新解读

密评及机构管理办法

《商用密码应用安全性评估管理办法》

规范商用密码应用安全性评估工作

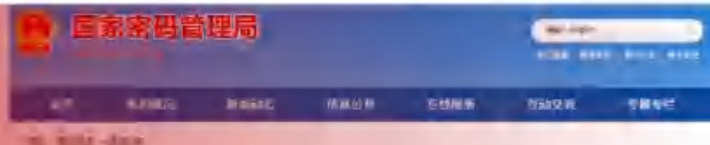


制定目的

2023年10月7日，国家密码管理局发布《商用密码应用安全性评估管理办法》（国家密码管理局令 第3号），自2023年11月1日起施行，旨在规范商用密码应用安全性评估工作，保障网络与信息安全，维护国家和社会公共利益，保护公民、法人和其他组织的合法权益。

《办法》制定的必要性

商用密码应用安全性评估 是加强和规范商用密码应用的重要抓手



国家密码管理局公告（第42号）
商用密码应用安全性评估试点机构目录
（共48家，以行政区划为序）

《中华人民共和国密码法》

颁布实施后，商用密码应用安全性评估制度依法确立，商用密码应用安全性评估机构纳入商用密码检测机构统一管理。

新修订《商用密码管理条例》

第三十八条、第四十一条进一步明确了商用密码应用安全性评估相关制度要求，为贯彻落实上位法规定，急需制定《办法》：

- 统筹细化商用密码应用安全性评估对象范围、责任主体、工作原则、程序内容、实施规范等规定；
- 依法规范商用密码应用安全性评估工作。

商用密码应用安全性评估试点

2017年以来，国家密码管理部门组织开展一系列商用密码应用安全性评估试点，在试点过程中，商用密码应用安全性评估的基本要求和思路做法已逐步得到相关管理部门、运营者和评估机构的认同，为《办法》的制定奠定了坚实的实践基础。

《办法》制定的总体思路



细化落实 “三同步一评估”要求

- 按照《密码法》、《条例》规定，《办法》对依法应当使用商用密码进行保护的重要网络与信息系统，明确要求同步规划、同步建设、同步运行商用密码保障系统，并定期进行商用密码应用安全性评估。
- 细化商用密码应用安全性评估要求，从规划、建设、运行各个阶段分别提出落实安排、明确评估程序及内容，建立起商用密码应用安全性评估制度的基本框架。



体现商用密码应用安全性评估系统性 原则

- 《办法》将商用密码应用方案评估、网络与信息系统运行前评估、网络与信息系统运行后定期评估统一纳入商用密码应用安全性评估工作体系
- 在实施中“按照同一套标准、遵循同一套程序、囊括同一套活动”，确保重要网络与信息系统全生命周期落实商用密码应用安全性评估要求。
- 将商用密码应用安全性评估机构统一纳入商用密码检测机构管理，进一步体现工作的系统性整体性。



明确商用密码应用安全性评估实施依据

- 按照《密码法》、《条例》关于运营者自行或者委托商用密码应用安全性评估机构开展评估的规定，《办法》分别明确了相关要求，并就两者需共同遵守的行为规范作出规定，从而明确了商用密码应用安全性评估活动的实施依据，有助于规范提升商用密码应用安全性评估工作质量。

《办法》主要内容

《办法》共21条

1.总体要求

1. **明确概念定义**，商用密码应用安全性评估是指按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。
2. **规定管理体制**，包括县级以上各级密码管理部门、国家机关和涉及商用密码工作的单位的监督管理职权。
3. **明确从业机构资质要求以及发展保障支持**。提出对商用密码应用安全性评估从业机构的资质要求，以及对商用密码应用安全性评估行业发展的保障支持。
4. 规定商用密码应用安全性评估的对象范围。

2.程序及内容要求

1. 规定“**三同步一评估**”的总体要求。
2. **明确不同阶段密评的程序要求**。重要网络与信息系统规划、建设、运行各阶段的商用密码应用安全性评估的程序要求。
3. **根据不同对象提出密评内容要求**。针对商用密码应用方案、网络与信息系统两类不同对象，分别提出商用密码应用安全性评估的内容要求。

3.实施规范

1. 规定开展商用密码应用安全性评估的通用行为规范和运营者委托开展评估的支持配合义务。
2. 规定运营者自行开展商用密码应用安全性评估的基本要求与行为规范。
3. 规定商用密码应用安全性评估结果备案制度。
4. 规定运营者开展应急处置的有关内容。

4.监督检查及法律责任

1. 规定了县级以上地方各级密码管理部门、国家机关和涉及商用密码工作的单位的监督检查职权。
2. 明确了运营者的违法情形及法律责任。
3. 规定了商用密码应用安全性评估管理人员的责任义务。

5.其他事项

规定了本办法实施的过渡安排和施行时间。

炼石整理：《商用密码应用安全性评估管理办法》总览

《商用密码应用安全性评估管理办法》

一、总体要求

1.立法目的

2.重要定义

3.监管机构的
监督管理职责

4.从业机构资质要求

5.支持鼓励密评产业发展

二、程序及内容要求

6.三同步一评估

7.重要网络与信息系统
规划阶段密评程序要
求

8.建设阶段
密评程序要求

9.建成运行后
密评程序要求

10.商密应用方案
密评内容要求

11.对已建成网络与信
息系统密评内容要求

三、实施规范

12.密评通用行为规范及
运营者委托开展评估的支持
配合义务

13.运营者自行开展密评的
基本要求与行为规范

14.结果备案制度

15.应急处置要求

四、监督检查及法律责任

16.监管专项检查

17.违反其他法规和本办法的行为处罚

18.违反本办法行为和处罚

19.监管人员违规行为和处分

五、其他事项

20.办法施行前正建和已运行系统要求

21.施行时间

贯彻落实上位法，保障网络与信息安全

1.总体要求

2.程序及内容要求

3.实施规范

4.监督检查及法律责任

5.其他事项

立法目的

- 为了规范商用密码应用安全性评估工作
- 保障网络与信息安全，维护国家安全和社会公共利益
- 保护公民、法人和其他组织的合法权益

制定依据

- 根据《中华人民共和国密码法》、《商用密码管理条例》等有关法律法规，制定本办法



本办法所称商用密码应用 安全性评估

是指按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。

商用密码应用安全性评估机构管理统一纳入商用密码检测机构管理

1.总体要求



国家密码管理局

- 负责管理**全国**的商用密码应用安全性评估工作
- 支持**商用密码应用安全性评估技术、标准、工具创新
- 完善**商用密码应用安全性评估标准体系
- 鼓励**设立商用密码应用安全性评估行业组织，加强行业自律，维护行业秩序

2.程序及内容要求



县级以上地方各级密码管理部门

- 负责管理**本行政区域**的商用密码应用安全性评估工作。

3.实施规范



国家机关和涉及商用密码工作的单位

- 在其职责范围内负责**指导、监督**本机关、本单位或者本系统的商用密码应用安全性评估工作。

4.监督检查及法律责任



评估机构

- 从事商用密码应用安全性评估活动，向社会出具**具有证明作用的商用密码应用安全性评估数据、结果的机构**，应当**经国家密码管理局认定**，依法**取得商用密码检测机构资质**。

5.其他事项

“重要网络与信息系统”纳入密评范围

法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统

以下 简称

重要网络与信息系统



其运营者

应当使用商用密码进行保护

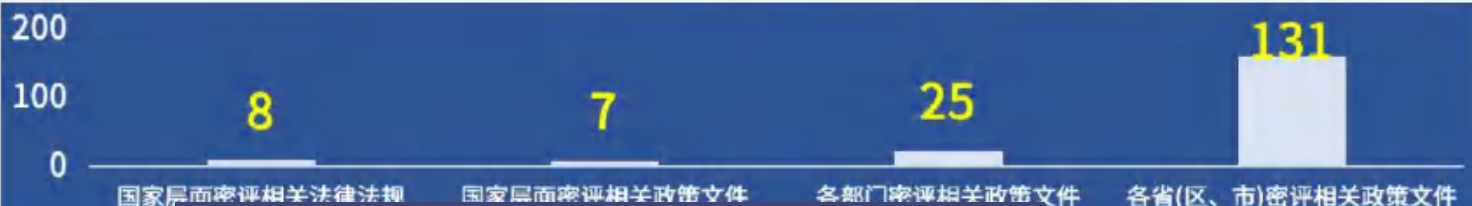


制定商用密码应用方案，配备必要的资金和专业人员

同步规划、同步建设、同步运行商用密码保障系统

并定期开展商用密码应用安全性评估

根据中国密码学会商用密码应用安全性评估联合委员会统计
截至2023年8月，密评相关法律法规、政策文件共计171项：



“重要网络与信息系统”如何界定？

1.总体要求

2017年4月22日起施行的《商用密码应用安全性评估管理办法（试行）》（注：该试行办法已被本次新发布的密评管理办法替代），曾明确定义：“重要领域网络和信息资源的重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础设施、网络安全等级保护第三级及以上信息系统。”

目前对“重要网络与信息系统”界定，依据是“法律、行政法规和国家有关规定”（可参考本幻灯篇第49-62页内容），涉及广泛的各行业、各领域重要信息系统：

2.程序及内容要求

3.实施规范



4.监督检查及法律责任



5.其他事项

细化重要网络与信息系统规划、建设、建成阶段的评估要求



商用密码应用方案开展应用安全性评估要求

1.总体要求

2.程序及内容要求

3.实施规范

4.监督检查及法律责任

5.其他事项

考量

考量商用密码应用需求的**全面性**、**合理性和针对性**，对照**相关标准规范**选取适用指标的**准确性**，以及**不适用指标论证的充分性**。

分析

分析商用密码应用**流程和机制**是否具备**可实施性**、**商用密码保护措施**是否达到相应的商用密码**应用要求**、**相关描述**是否详尽。

编制

编制形成商用密码应用安全性评估报告。

论证

论证**商用密码技术、产品和服务**选用的**合规性**，**密钥管理的安全性**，以及使用商用密码**解决安全风险的科学性**。



对建设完成的网络与信息系统开展商用密码应用安全性评估要求



运营者以合规为前提开展商用密码应用安全性评估活动

1.总体要求



运营者

开展商用密码应用安全性评估活动

应当遵守**法律法规、标准规范要求**，遵循**客观实际、科学公正、诚实信用**原则

2.程序及内容要求

委托商用密码检测机构开展商用密码应用安全性评估，**不得对**评估结果施加**不当**影响，并应当提供以下支持：

3.实施规范

重要数据备份	设备清单和网络拓扑	运营维护记录	管理入口	管理员	其他事项
对 网络与信息系统 的重要数据进行备份；	提供 完整有效的网络与信息系统设备清单和网络拓扑 ；	提供详细的 网络与信息系统商用密码应用方案、密码相关管理制度和密码配置、运行、维护记录	提供商用密码产品 管理入口、网络交换设备接入端口等相关信息、数据接入分析条件 ，并配合进行数据留存；	安排网络与信息系统相关网络管理员、系统管理员、 密钥管理员、密码安全审计员、密码操作员 等做好配合；	其他需要配合的事项。

4.监督检查及法律责任

5.其他事项

运营者自行开展网络与信息系统展商用密码应用安全性评估的要求

1.总体要求

自行开展商用密码应用安全性评估的网络与信息系统，其运营者应当符合以下要求：

2.程序及内容要求

具有与开展商用密码应用安全性评估活动相适应的设备设施；

具有与开展商用密码应用安全性评估活动相适应的项目管理、质量管理、人员管理、档案管理、安全保密管理等规章制度；

具有与开展商用密码应用安全性评估活动相适应的专业人员；

具有与开展商用密码应用安全性评估活动相适应的专业能力。

3.实施规范



自行开展商用密码应用安全性评估形成的商用密码应用安全性评估报告

应当符合

相关国家标准、行业标准和有关规定的要求

其他要求



由本单位密码或者网络安全负责人签字确认并加盖本单位公章。

4.监督检查及法律责任

5.其他事项

注意：运营者应当对商用密码应用安全性评估原始记录和商用密码应用安全性评估报告归档留存，保证其具有可追溯性。商用密

重要网络与信息系统运营者应向管理部门备案评估报告

1.总体要求

2.程序及内容要求

3.实施规范

4.监督检查及法律责任

5.其他事项



注意：省、自治区、

更多免费行业报告

并购买

www.ipopo.cn

评估工作开展情况。

密码相关重大事件必要时启动应急处置方案

1.总体要求

2.程序及内容要求

3.实施规范

4.监督检查及法律
责任

5.其他事项

实施规范

密码相关重大事件

运营者发现**密码相关重大安全事件、重大密码安全隐患或者特殊紧急情况**的，应当及时向**国家密码管理局或者网络与信息系统所在地省、自治区、直辖市密码管理部门报告**，并**启动应急处置方案**，**必要时开展商用密码应用安全性评估**。

监督及法律责任

专项检查

县级以上地方各级密码管理部门、国家机关和涉及商用密码工作的单位可以根据工作需要，对本地区、本机关、本单位或者本系统的重要网络与信息系统商用密码应用安全性评估情况**开展专项检查**。

重要网络与信息系统运营者法律责任

	主体	违法行为	处罚
1.总体要求	重要网络与信息系统的运营者	(一) 重要网络与信息系统规划阶段, 未对商用密码应用方案进行商用密码应用安全性评估的;	有以上情形之一的, 由密码管理部门责令改正, 给予警告; 拒不改正或者有其他严重情节的, 处10万元以上100万元以下罚款, 对直接负责的主管人员处1万元以上10万元以下罚款。
2.程序及内容要求		(二) 重要网络与信息系统建设阶段, 未按照通过商用密码应用安全性评估的商用密码应用方案建设商用密码保障系统的;	
3.实施规范		(三) 重要网络与信息系统运行前, 未开展商用密码应用安全性评估的;	
		(四) 重要网络与信息系统运行前, 未通过商用密码应用安全性评估且未进行改造的;	
		(五) 重要网络与信息系统建成运行后, 未定期开展商用密码应用安全性评估的;	
		(六) 重要网络与信息系统建成运行后, 未通过定期开展的商用密码应用安全性评估且未进行改造的;	
4.监督检查及法律责任		(七) 违反法律法规、标准规范要求开展商用密码应用安全性评估的;	
		(八) 不符合相关要求自行开展商用密码应用安全性评估的。	
5.其他事项	违反本办法规定	(一) 对商用密码应用安全性评估结果施加不当影响的; (二) 未为商用密码应用安全性评估活动提供必要支持的; (三) 未按照要求进行商用密码应用安全性评估结果备案的。	有以上情形之一的, 由密码管理部门责令改正; 逾期未改正或者改正后仍不符合要求的, 处1万元以上10万元以下罚款, 对直接负责的主管人员处5000元以上5万元以下罚款。
	从事商用密码应用安全性评估监督管理工作的人员	滥用职权、玩忽职守、徇私舞弊, 或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息	依法给予处分。

正建和已运行的重要网络与信息系统的评估要求

1.总体要求

施行前正建

本办法**施行前正在建设的重要网络与信息系统**，其运营者应当加强商用密码应用方案编制论证，建设完善商用密码保障系统，并按照本办法**第八条规定**开展商用密码应用安全性评估。

2.程序及内容要求

3.实施规范

施行前已运行

本办法**施行前已经投入运行的重要网络与信息系统**，其运营者应当按照本办法**第九条**规定开展商用密码应用安全性评估。

4.监督检查及法律责任

5.其他事项



本办法自2023年11月1日起施行。

更新解读

密评及机构管理办法

《商用密码检测机构管理办法》

加强密评机构管理，规范商用密码检测活动



制定目的

2023年10月7日，国家密码管理局发布商用密码检测机构管理办法（国家密码管理局令 第2号），自2023年11月1日起施行，旨在加强商用密码检测机构管理，规范商用密码检测活动。

第一条 为了加强商用密码检测机构管理，规范商用密码检测活动，根据《中华人民共和国密码法》、《商用密码管理条例》等有关法律法规，制定本办法。

更多免费行业报告

并购买

www.ipopo.cn

办法制定是贯彻落实党中央、国务院关于商密管理决策部署的必然要求

《商用密码检测机构管理办法》制定

必然要求

是贯彻落实党中央、国务院关于商用密码管理决策部署的必然要求

重要举措

是深化行政审批制度改革、优化营商环境的重要举措

迫切需求

是规范商用密码检测机构管理的迫切需要

2019年10月,《中华人民共和国密码法》正式发布,提出了“商用密码检测、认证机构应当依法取得相关资质,并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证”的要求。

新修订的《条例》第十三条规定:“从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动,向社会出具具有证明作用的数据、结果的机构,应当经国家密码管理部门认定,依法取得商用密码检测机构资质。”

为有效贯彻落实上位法规定,按照商用密码依法管理要求,有必要制定《办法》,细化商用密码检测机构管理措施。

近年来,党中央、国务院围绕深化行政审批制度改革、优化营商环境作出了一系列重大决策部署。

为严格落实行政审批制度改革要求,有必要制定《办法》,优化审批流程,规范审批条件,为保护市场主体权益,净化市场环境,优化政务服务,规范监管执法提供法治保障和政策支持。

随着商用密码产业的持续发展和应用需求的不断提升,商用密码检测需求显著增加,急需出台专门规章进一步规范商用密码检测机构管理工作。

《办法》根据商用密码检测机构管理现实需要,对检测机构资质认定、监督管理等提出明确要求,对于规范检测机构市场准入及从业行为、促进商用密码检测行业健康发展具有重要意义。

《商用密码检测机构管理办法》制定总体思路

《商用密码检测机构管理办法》制定



坚持依法管理	坚持公平公正	坚持保障安全 and 创新发展相统一
严格依据《密码法》、《条例》及相关法律法规中商用密码检测相关管理要求，制定商用密码检测机构管理各项措施。	系统设计商用密码检测机构管理体系，<u>细化明确商用密码检测活动要求</u>，<u>严格规范检测机构从业行为</u>。	按照<u>既满足商用密码检测安全需要，又鼓励商用密码检测机构创新发展、做大做强</u>的导向，科学设置检测机构准入条件和监督管理措施。

《商用密码检测机构管理办法》主要内容

《商用密码检测机构管理办法》共29条

1. 总体要求

1. 规定适用范围，包括商用密码产品检测机构和商用密码应用安全性评估机构的资质认定和监督管理。
2. 明确监管体制，国家密码管理局负责全国商用密码检测机构的资质认定和监督管理。县级以上地方各级密码管理部门负责本行政区域内商用密码检测机构的监督管理。

2. 资质认定条件和程序

1. 明确商用密码检测机构资质认定的规范依据。
2. 规定资质认定的条件要求。
3. 规定资质认定的程序，包括申请、受理、审查、决定、颁证等环节。
4. 规定资质变更、延续、注销等相关要求。

3. 从业规范

1. 明确了商用密码检测机构及相关从业人员应遵守的行为规范。
2. 针对检测报告、数据和样品管理、信息报送、检测行为等方面对检测活动提出具体要求。

4. 监督检查及法律责任

1. 规定了密码管理部门的监督检查职权及结果处理。
2. 明确了商用密码检测机构的违法情形及法律责任。
3. 规定了商用密码检测机构监督管理信息公示和管理人员的责任义务。

5. 其他事项

炼石整理：《商用密码检测机构管理办法》总览

商用密码检测机构管理办法

一、立法目的

1.立法目的

2.适用范围

3.检测机构认定

4.监督管理

5.检测机构义务

二、资质认定条件和程序

6.认定条件

7-11.认定程序

12.资质证书

13.资质变更

14.资质注销

三、从业规范

15.检测基本要求

16.符合资质认定

17.检测机构从业要求

18.检测报告要求

19.检测信息管理要求

20.工作报告及数据报送

21.禁止虚假检测

四、监督检查

22.监督检查职权范围

23.监督检查结果处理

五、法律责任

24.不正当手段法律责任

25.26.违法情形及法律责任

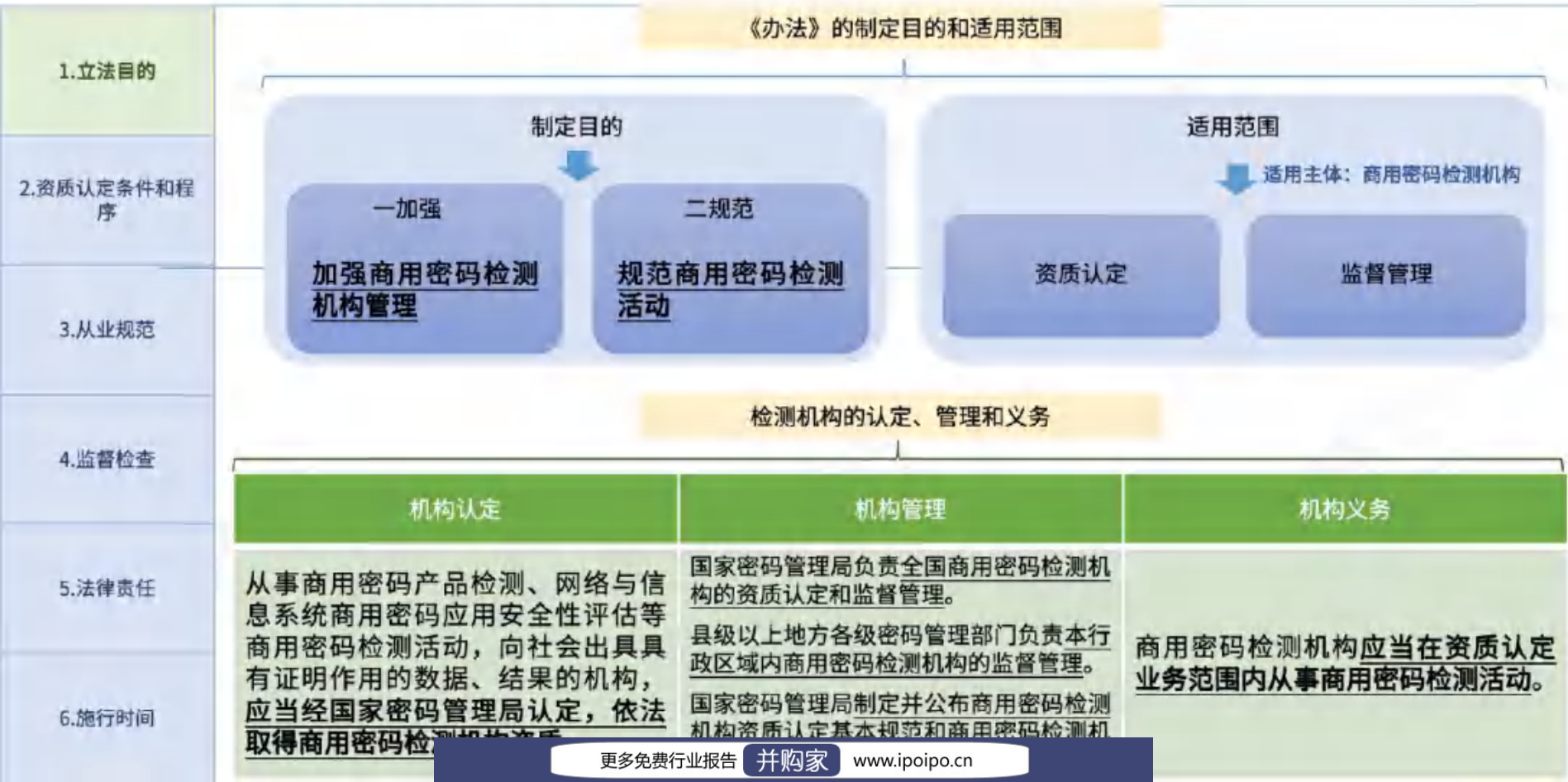
27.监督管理信息公示

28.监管人员违规处罚

六、施行时间

29.施行日期

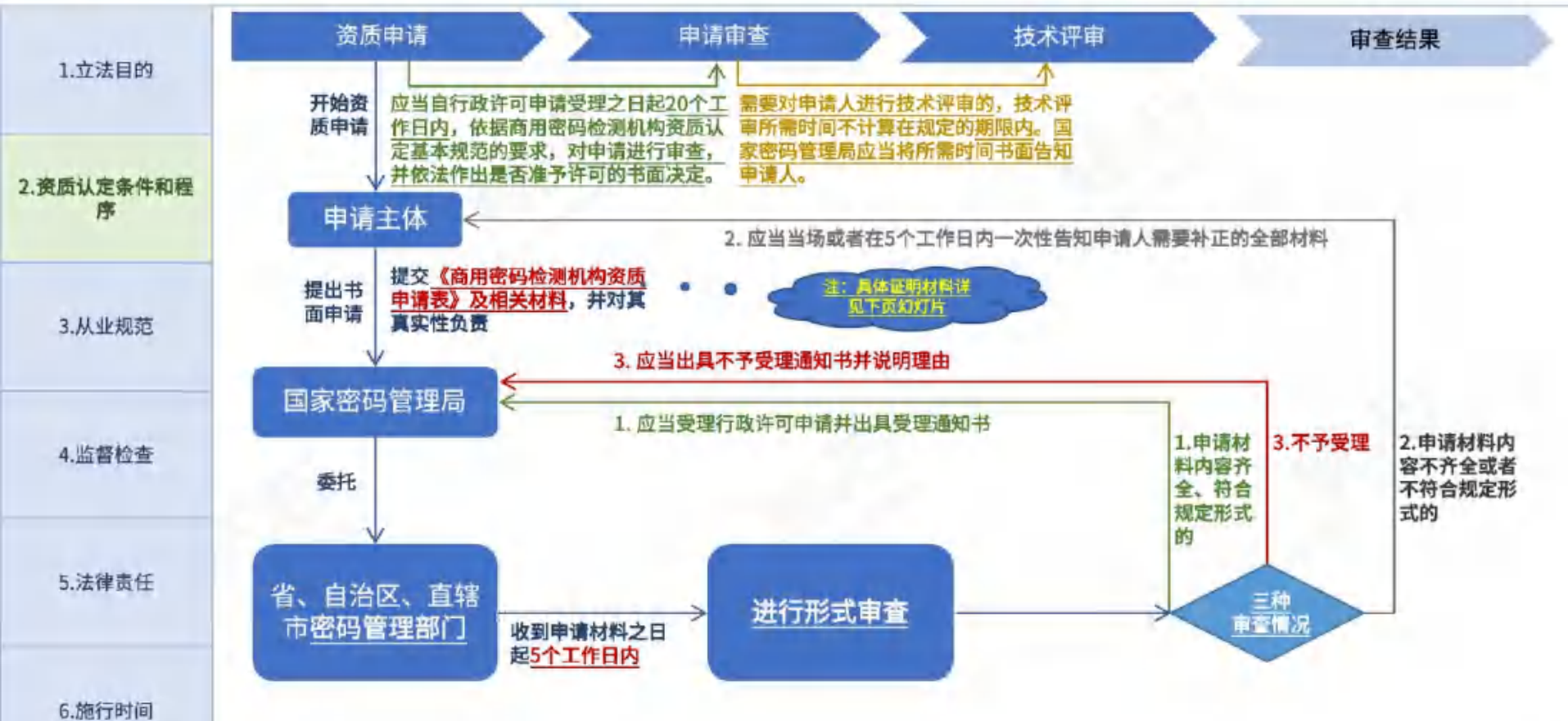
办法制定将加强机构管理以及规范商密检测活动



资质申请需在人力、物力、技术、管理等维度满足要求

1.立法目的	取得商用密码检测机构资质，应当符合下列条件	
2.资质认定条件和程序	(一)	具有 <u>法人资格</u>
	(二)	具有与从事商用密码检测活动相适应的 <u>资金</u>
3.从业规范	(三)	<u>成立2年以上</u> ，从事网络安全检测评估领域相关工作 <u>1年以上</u> ， <u>无重大违法或者不良信用记录</u>
	(四)	具有与从事商用密码检测活动相适应的 <u>场所</u>
4.监督检查	(五)	具有与从事商用密码检测活动相适应的 <u>设备设施</u>
	(六)	具有保证商用密码检测活动 <u>独立、公正、科学、诚信</u> 的管理体系
5.法律责任	(七)	具有与从事商用密码检测活动相适应的 <u>专业人员</u>
	(八)	具有与从事商用密码检测活动相适应的 <u>专业能力</u>
6.施行时间	特殊情况： 外商投资企业法人申请商用密码检测机构资质，除符合上述条件外，还 <u>应当符合我国外商投资有关法律</u>	

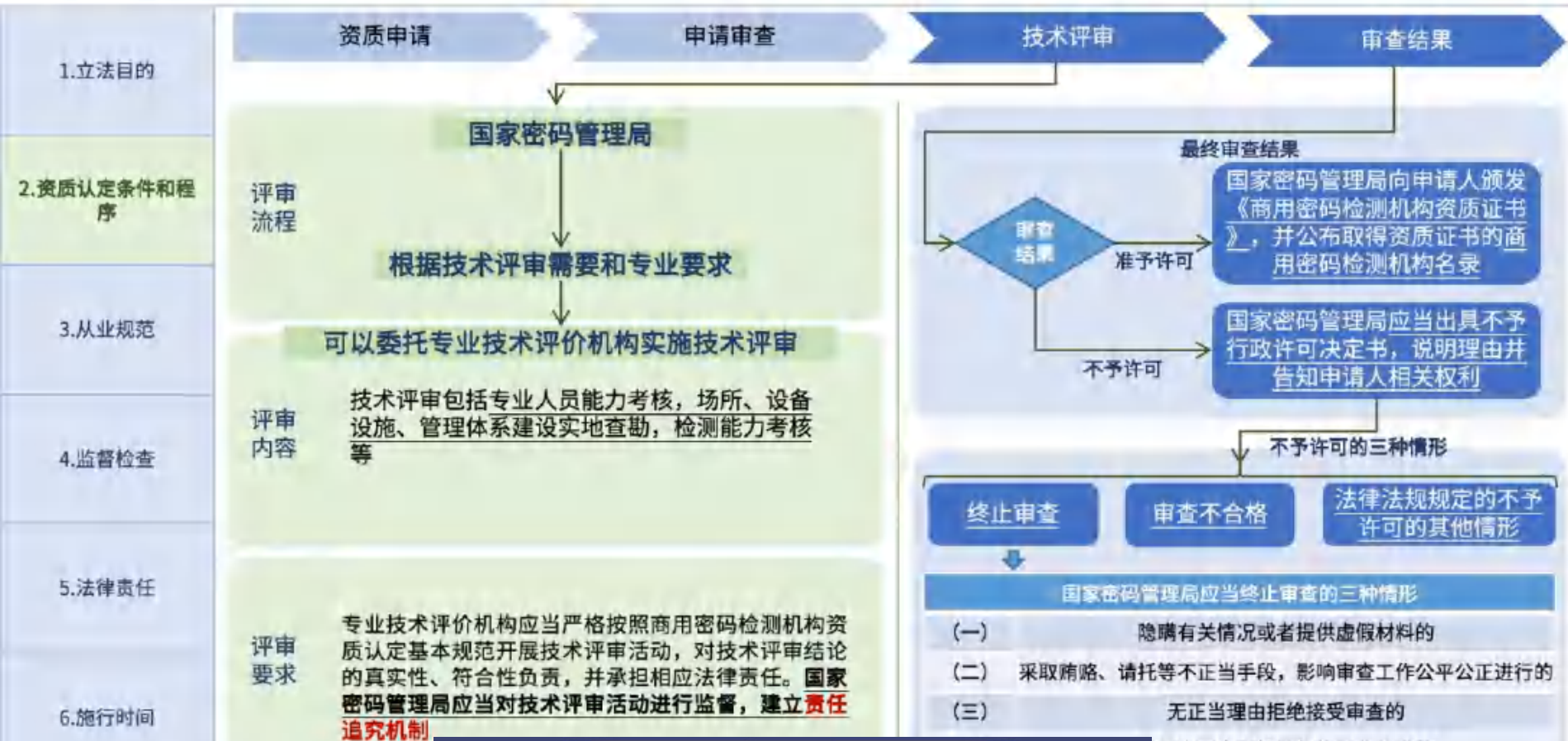
申请商用密码检测机构资质应当向国家密码管理局提出书面申请



资质申请时需要提交的相关材料列表

	资质申请	申请审查	技术评审	审查结果
1.立法目的	资质申请 ↓ 资质申请时需要提交的相关材料列表			
2.资质认定条件和程序	相关材料			
	(一)	法人资格证书		
	(二)	资本结构和股权情况		
3.从业规范	(三)	无重大违法或者不良信用记录、不从事可能影响商用密码检测公平公正性活动的承诺		
	(四)	工作场所等固定资产产权证书或者租赁合同		
	(五)	工作环境和设备设施配置情况		
	(六)	项目管理、质量管理、人员管理、档案管理、安全保密管理等管理体系建立情况		
5.法律责任	(七)	法定代表人、最高管理者、技术负责人、质量负责人、授权签字人以及专业人员情况		
	(八)	申请人认为需要补充的其他材料		
6.施行时间				

国家密码管理局可以委托专业技术评价机构实施技术评审



有效期届满需要延续的应当在有效期届满3个月前提出书面申请

1.立法目的

2.资质认定条件和程序

3.从业规范

4.监督检查

5.法律责任

6.施行时间

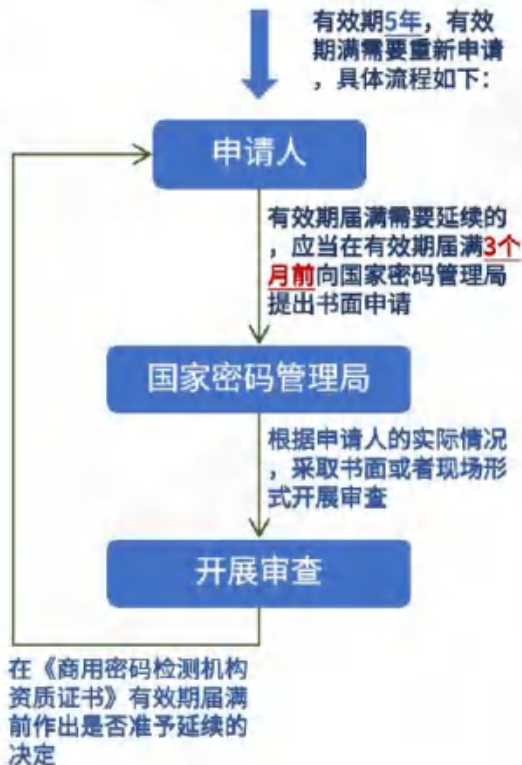
证书内容

证书内容列表

- | | |
|-----|----------|
| (一) | 获证机构名称 |
| (二) | 统一社会信用代码 |
| (三) | 注册地址 |
| (四) | 证书编号 |
| (五) | 有效期限 |
| (六) | 资质认定业务范围 |
| (七) | 发证机关 |
| (八) | 发证日期 |

证书有效期

有效期5年，有效期届满需要重新申请，具体流程如下：



禁止情形

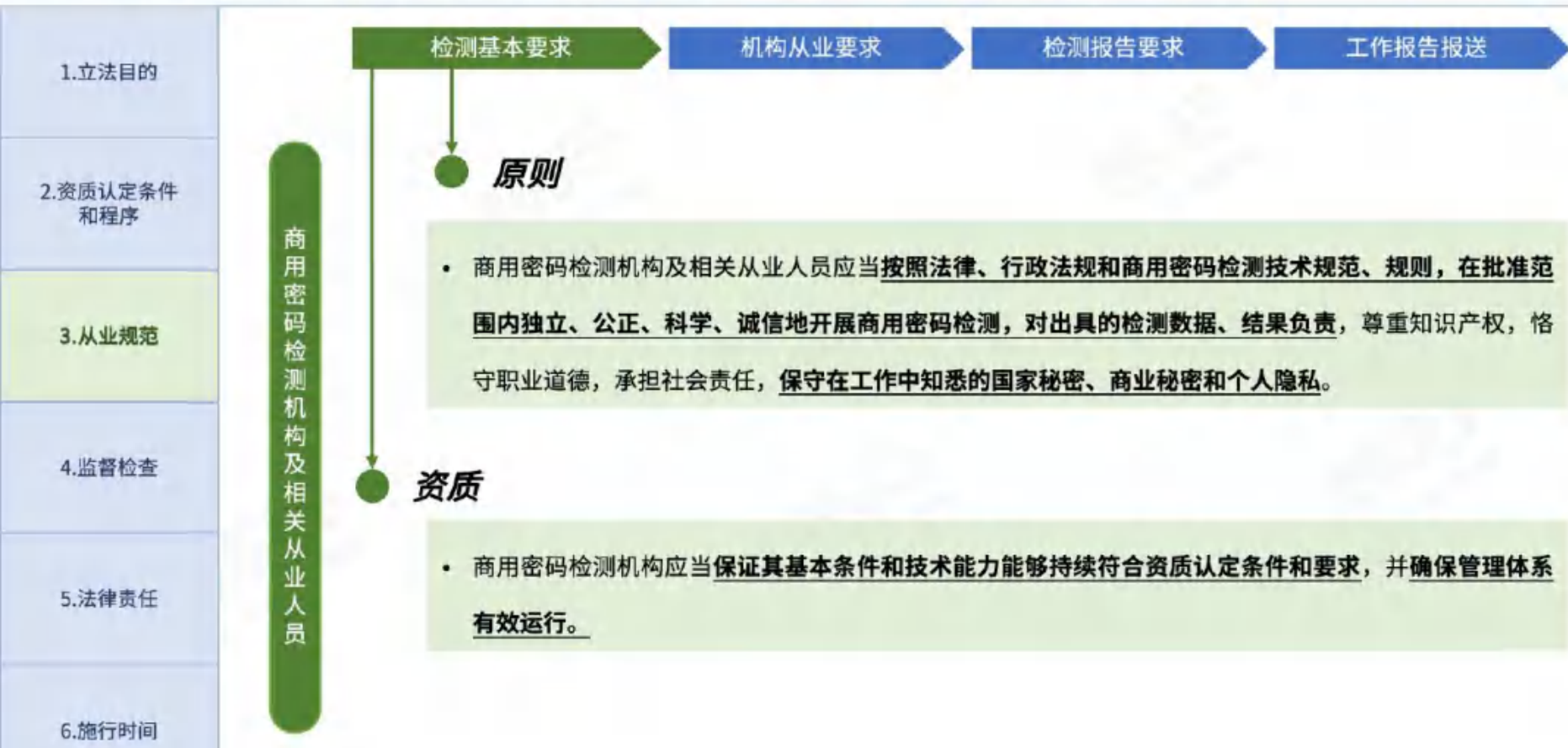
证书禁止情形

- | | |
|-----|----|
| (一) | 转让 |
| (二) | 出租 |
| (三) | 出借 |
| (四) | 伪造 |
| (五) | 变造 |
| (六) | 冒用 |
| (七) | 租借 |

商用密码检测机构资质变更及注销的具体情况表

	资质变更	资质注销
1.立法目的		
2.资质认定条件和程序	有下列情形之一的，商用密码检测机构应当自变更之日起30日内向国家密码管理局申请办理变更手续： (一) 机构名称、注册地址、法人性质发生变更的 (二) 法定代表人、最高管理者、技术负责人、质量负责人、授权签字人发生变更的 (三) 资质认定业务范围发生变更的 (四) 依法需要办理变更的其他事项 注：商用密码检测机构发生变更的事项影响其符合资质认定条件和要求的，国家密码管理局根据申请人的实际情况，采取书面或者现场形式开展审查。需要进行技术评审的，依照本办法第九条规定对其开展技术评审。	商用密码检测机构有下列情形之一的，国家密码管理局应当依法注销其商用密码检测机构资质： (一) 《商用密码检测机构资质证书》有效期届满，未申请延续或者依法不予延续批准的 (二) 申请注销商用密码检测机构资质的 (三) 被依法撤销、吊销商用密码检测机构资质的 (四) 依法终止的 (五) 因法人性质变更、改制、分立或者合并等原因发生变化，或者发生其他影响其符合资质认定条件和要求的变更事项，经审查发现不符合资质认定条件和要求的 (六) 资质认定业务范围被全部取消的 (六) 法律法规规定的应当注销商用密码检测机构资质的其他情形
3.从业规范		
4.监督检查		
5.法律责任		
6.施行时间		

在批准范围内独立、公正、科学、诚信地开展商用密码检测



明确八项商用密码检测机构从业要求

商用密码检测机构

1.立法目的

检测基本要求

机构从业要求

检测报告要求

工作报告报送

2.资质认定条件和程序

3.从业规范

4.监督检查

5.法律责任

6.施行时间



安全保密教育和业务培训

- 加强对本机构人员的监督管理，经常性组织开展安全保密教育和业务培训；本机构从事检测活动的专业人员每年接受商用密码教育培训的时长不得少于40学时，相关情况应当记录留存；



不得从事影响检测公平公正活动

- 本机构及关联方不得从事商用密码产品生产、销售（检测工具除外），信息系统或者商用密码保障系统集成、运营，电子认证服务，电子政务电子认证服务，或者其他可能影响商用密码检测公平公正性的活动；



不得恶意竞争

- 不得同时聘用正在其他商用密码检测机构从业的人员，或者存在其他恶意竞争、扰乱市场秩序的情形；



承担业务要求

- 不得以单独出租设备设施或者委派人员等方式承担业务，所承担的业务不得分包、转包；



禁止推荐/限定特定主体产品服务

- 不得以任何方式推荐或者限定被检测单位购买使用特定主体生产或者提供的商用密码产品或者服务；



独立于利益相关各方

- 独立于出具的检测数据、结果、报告所涉及的利益相关各方，不受任何可能干扰技术判断因素的影响；



设备设施要求

- 使用符合国家密码管理要求的设备设施；



其他要求

- 法律法规和国家有关规定提出的其他从业要求。

明确检测报告要求及工作报告报送规范



每年1月15日前

商用密码检测机构不得出具虚假或者失实检测数据、结果、报告

1.立法目的

2.资质认定条件和程序

3.从业规范

4.监督检查

5.法律责任

6.施行时间

禁止造假/
失实检测

商用密码检测机构不得有以下出具虚假或者失实检测数据、结果、报告的行为：

- **【未检测】** 未经检测，直接出具检测数据、结果、报告的；
- **【篡改编造】** 篡改、编造原始数据、记录，出具检测数据、结果、报告的；
- **【伪造或非授权签发】** 伪造检测报告和原始记录签名，或者非授权签字人签发检测报告的；
- **【漏检、干扰或改动】** 漏检关键项目、干扰检测过程或者改动关键项目的检测方法，造成检测数据、结果、报告失实的；
- **【其他】** 其他出具虚假或者失实检测数据、结果、报告的行为。

国家密码管理局、密码管理部门开展监督检查职权及结果处理

1.立法目的

2.资质认定条件和程序

3.从业规范

4.监督检查

5.法律责任

6.施行时间

国家密码管理局

根据工作需要

行使职权

密码管理部门对商用密码检测机构依法开展监督检查，可以行使下列职权：

- **【现场检查】** 进入检测活动场所实施现场检查；
- **【调查了解/验证】** 向商用密码检测机构、委托人等有关单位及人员调查、了解有关情况或者验证相关检测活动；
- **【查阅复制】** 查阅、复制有关合同、票据、账簿以及检测活动中形成的检测数据、结果、报告等有关材料；

密码管理部门

依法开展
监督检查

积极
配合

商用密码检测机构

国家密码管理局根据工作需要，可以行使下列职权：

- **【检测能力验证】** 组织商用密码检测机构检测能力验证；
- **【检测材料抽样检查】** 对商用密码检测机构出具的检测数据、结果、报告等有关材料进行抽样检查。

商用密码检测机构应当积极配合密码管理部门的监督检查，按照要求参加检测能力验证和抽样检查，并如实提供相关材料和信息。

- **【检测能力验证/抽样检查结果不合格】** 应当开展为期不少于6个月的整改，整改期间不得开展相应业务范围的商用密码检测活动。
- **【整改合格】** 商用密码检测机构整改结束后，应当经国家密码管理局组织验收合格，方可恢复开展相应业务范围的商用密码检测活动；
- **【整改仍不满足要求】** 经整改仍不能满足相应业务范围的资质认定条件和要求的，取消其相应业务范围的资质认定，直至注销其商用密码检测机构资质。

监管落实商用密码检测机构法律责任¹

	违规事项	监管部门	处罚详情
1.立法目的	以 <u>欺骗、贿赂等不正当手段</u> 取得商用密码检测机构资质的	国家密码管理局	- 依法撤销商用密码检测机构资质 - 该机构在3年内不得再次申请商用密码检测机构资质
2.资质认定条件和程序	申请商用密码检测机构资质时 <u>隐瞒有关情况或者提供虚假材料</u> 的		- 不予受理或者不予许可 - 该机构在1年内不得再次申请商用密码检测机构资质
3.从业规范	商用密码检测机构违反《中华人民共和国密码法》、《商用密码管理条例》和本办法规定，有下列情形之一的： - 超出批准范围开展商用密码检测的； - 转让、出租、出借、伪造、变造、冒用、租借《商用密码检测机构资质证书》的； - 本机构及关联方从事商用密码产品生产、销售（检测工具除外），信息系统或者商用密码保障系统集成、运营，电子认证服务，电子政务电子认证服务；或者其他可能影响商用密码检测公平公正性的活动的； - 同时聘用正在其他商用密码检测机构从业的人员或者存在其他恶意竞争、扰乱市场秩序情形的； - 以单独出租设备设施或者委派人员等方式承担业务，或者分包、转包所承担业务的； - 推荐或者限定被检测单位购买使用特定主体生产或者提供的商用密码产品或者服务的； - 违反法律、行政法规和商用密码检测技术规范、规则要求开展检测活动或者存在其他影响检测独立、公正、科学、诚信的行为的； - 出具的检测数据、结果、报告虚假或者失实的； - 未按照要求如实报送年度工作报告以及相关统计数据的； - 泄露在工作中知悉	密码管理部门	- 责令限期整改 - 责令改正或者停止违法行为，给予警告，没收违法所得 - 违法所得30万元以上的，可以并处违法所得1倍以上3倍以下罚款 - 没有违法所得或者违法所得不足30万元的，可以并处10万元以上30万元以下罚款
4.监督检查			
5.法律责任		国家密码管理局	情节严重的，由国家密码管理局吊销其商用密码检测机构资质
6.施行时间			

监管落实商用密码检测机构法律责任²

	违规事项	监管部门	处罚详情
1.立法目的	商用密码检测机构违反本办法规定，有下列情形之一的：		
2.资质认定条件和程序	- 未按照要求申请办理变更手续的； - 未按照要求开展安全保密教育和业务培训的； - 使用不符合国家密码管理要求的设备设施的； - 出具未经授权签字人签字确认的检测报告，授权签字人超出其业务能力范围签发检测报告，或者未在检测报告上加盖机构公章或者专用章的； - 未按照要求保存检测原始记录和检测报告，或者未按照要求妥善保管检测样品和相关数据信息的。	密码管理部门	<u>责令改正</u> <u>逾期未改正或者改正后仍不符合要求的，处1万元以上10万元以下罚款</u>
3.从业规范			
4.监督检查	—	县级以上地方各级密码管理部门	<u>依法公开监督检查结果</u>，将商用密码检测机构受到的<u>行政处罚等信息</u>纳入国家企业信用信息公示系统等平台 <u>定期将年度商用密码检测机构监督检查结果等信息逐级报至国家密码管理局</u>
5.法律责任			
6.施行时间	从事商用密码检测机构监督管理工作的人员滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的	—	<u>依法给予处分</u>

*本办法自2023年11月1日起施行

01 密评背景介绍

02 密评总体要求

03 密评测评要求

04 密评方案要求

05 密评测评过程

06 密评团标解读

07 密改FAQ解读

08 密改方案实践



总体概览



信息安全技术 信息系统密码应用基本要求
GB/T 39786-2021

信息系统密码应用
测评过程指南
GB/T 0116-2021

信息系统密码应用高
风险判定指引

商用密码应用安全性
评估量化评估规则



贯彻落实《密码法》，指导商用密码应用与安全性评估工作的基础性标准



2021年3月9日，国家市场监管总局、国家标准化管理委员会发布公告，正式发布**国家标准GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》**，于2021年10月1日起实施，旨在：

指导、规范信息系统密码应用的规划、建设、运行及测评，对于规范和引导信息系统合规、正确、有效应用密码，切实维护国家网络与信息安全具有重要意义。

在本标准的基础之上，各领域与行业可结合本领域与行业的密码应用需求，来指导、规范信息系统密码应用。



界定重要定义

引用GB/T 37092 《信息安全技术 密码模块安全要求》

机密性Confidentiality

保证信息不被泄露给非授权实体的性质。

数据完整性Data Integrity

数据没有遭受以非授权方式所作的改变的性质。

真实性Authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息之类的实体。

不可否认性Non-Repudiation

证明一个已经发生的操作行为无法否认的性质。

加密 Encipherment ; Encryption

对数据进行密码变换以产生密文的过程。

身份鉴别 Identity Authentication

证实一个实体所声称身份的过程。

访问控制 Access Control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生存周期的管理。

消息鉴别码 Message Authentication Code

利用对称密码技术或密码杂凑技术，在秘密密钥参与下，由消息所导出的数据项。任何持有这一秘密密钥的实体，可利用消息鉴别码检查消息的完整性和始发者身份。

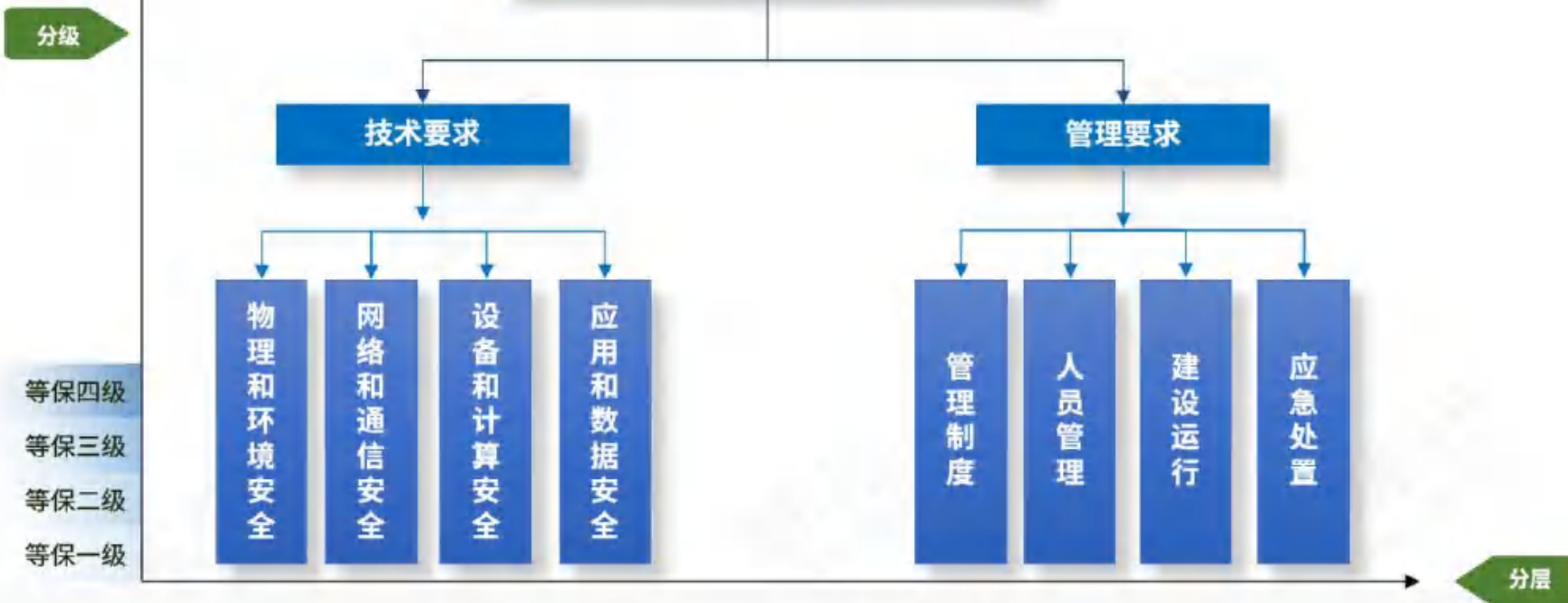
动态口令One-Time Password

基于时间、事件等方式动态生成的一次性口令。

密钥Key

控制密码算法运算的关键信息或参数。

测评要求



• 评估原则

遵循商用密码管理政策和GB/T39786-2021《信息系统密码应用基本要求》、《信息系统密码测评要求》等相关密码标准的要求，遵循独立客观、公正的原则。

• 评估内容

主要对物理和环境、网络和通信、设备和计算、应用和数据四个技术层面，以及管理制度、人员管理、建设运行、应急处置四个管理层面进行测评。

注：第5级密码应

更多免费行业报告

并购家

www.ipopo.cn

本标准中描述。

技术和管理要求维度涉及的保护对象

技术要求

技术要求主要由机密性、完整性、真实性、不可否认性4个密码安全功能维度构成，具体保护对象或应用场景描述如下：

机密性技术要求保护对象

使用密码技术的加解密功能实现机密性

- 身份鉴别信息
- 密钥数据
- 传输的重要数据
- 信息系统应用中所有存储的重要数据

完整性技术要求保护对象

使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现完整性

- 身份鉴别信息
- 密钥数据
- 日志记录
- 访问控制信息
- 重要信息资源安全标记
- 重要可执行程序
- 视频监控录像记录
- 电子门禁系统进出记录
- 传输的重要数据
- 信息系统应用中所有存储的重要数据

真实性技术要求应用场景

使用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现真实性

- 进入重要物理区域人员的身份鉴别
- 通信双方的身份鉴别
- 网络设备接入时的身份鉴别
- 重要可执行程序的来源真实性保证
- 登录操作系统和数据库系统的用户身份鉴别
- 应用系统的用户身份鉴别

不可否认性技术要求 保护对象

使用基于公钥密码算法的数字签名机制等密码技术来保证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。

管理要求

管理要求由管理制度、人员管理、建设运行、应急处置等4个密码应用管理维度构成，具体如下：

管理制度

密码应用安全管理相关流程制度的制定、发布、修订的规范性要求

人员管理

密码相关安全人员的密码安全意识以及关键密码安全岗位员工的密码安全能力的培养、人员工作流程要求等

建设运行

建设运行过程中密码应用安全要求及方案落地执行的一致性和有效性要求

应急处置

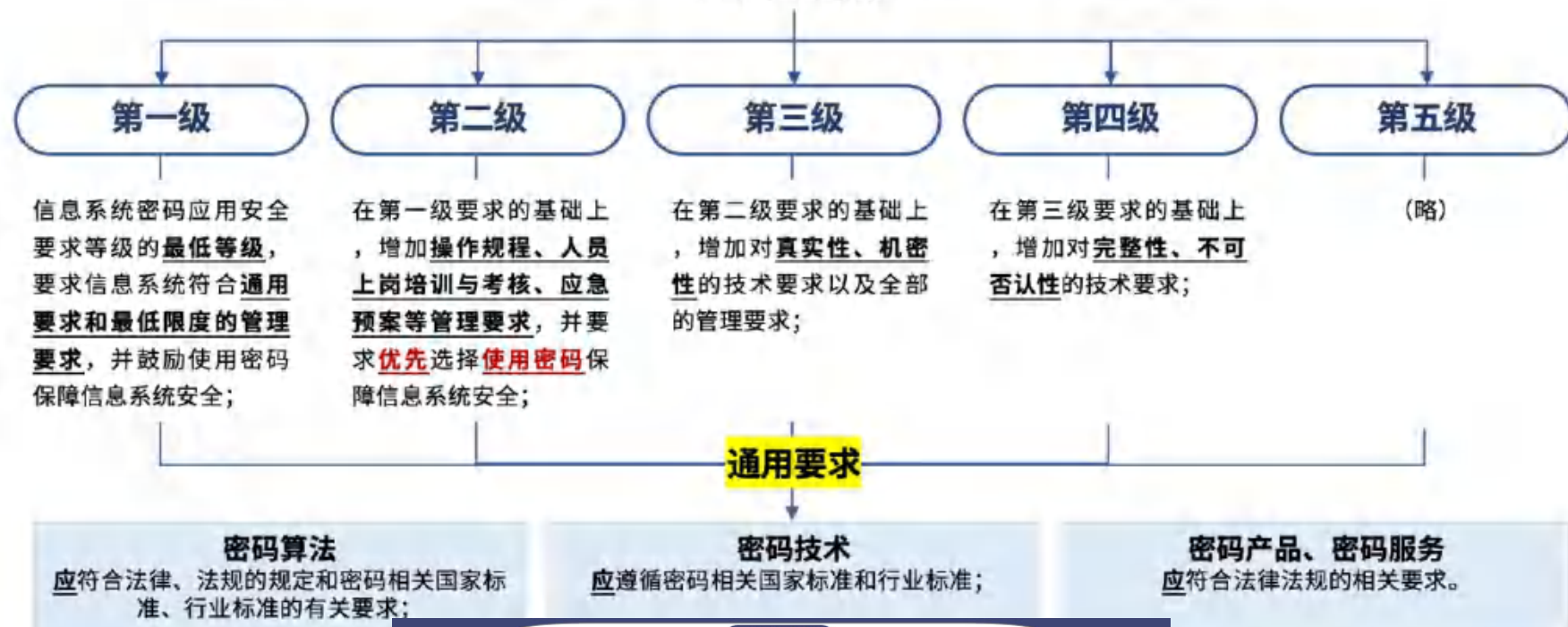
处理密码应用安全相关的应急突发事件的能力要求

密码应用基本要求等级

信息系统密码应用等级

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



物理和环境安全指标体系

1.物理和环境安全	物理和环境安全-指标体系	一级	二级	三级	四级
2.网络和通信安全	采用密码技术进行物理访问 <u>身份鉴别</u> ，保证重要区域进入人员身份真实性	可	宜	宜	应
3.设备和计算安全	采用密码技术保证 <u>电子门禁系统</u> 进出记录数据存储完整性	可	可	宜	应
4.应用和数据安全	采用密码技术保证 <u>视频监控音像记录数据存储完整性</u>	—	—	宜	应
5.管理制度	以上采用的 <u>密码产品</u> ，应达到GB/T 37092相应的安全要求	—	应一级以上	应二级以上	应三级以上
6.人员管理	以上如采用 <u>密码服务</u> ，该密码服务应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	应	应	应	应
7.建设运行					
8.应急处置					

网络和通信安全指标体系

	网络和通信安全-指标体系	一级	二级	三级	四级
1.物理和环境安全					
2.网络和通信安全	采用密码技术对通信实体进行（4级：双向） <u>身份鉴别</u> ，保证通信实体身份的真实性	可	宜	应	应
3.设备和计算安全	采用密码技术保证 <u>通信过程中数据的完整性</u>	可	可	宜	应
4.应用和数据安全	采用密码技术保证 <u>通信过程中重要数据的机密性</u>	可	宜	应	应
	采用密码技术保证 <u>网络边界访问控制信息的完整性</u>	可	可	宜	应
5.管理制度	以上采用的 <u>密码产品</u> ，应达到GB/T 37092相应的安全要求	—	应一级以上	应二级以上	应三级以上
6.人员管理	采用密码对从外部连接到内部网络的设备进行 <u>接入认证</u> ，确保接入的设备身份真实性	—	—	可	宜
7.建设运行	以上如采用 <u>密码服务</u> ，该密码服务应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	应	应	应	应
8.应急处置					

设备和计算安全指标体系

	设备和计算安全-指标体系	一级	二级	三级	四级
1.物理和环境安全	采用密码技术对登录设备的用户进行 <u>身份鉴别</u> ，保证用户身份的真实性	可	宜	应	应
2.网络和通信安全	采用密码技术保证 <u>日志记录的完整性</u>	可	可	宜	应
3.设备和计算安全	远程管理设备时，采用密码技术建立 <u>安全的信息传输通道</u>	—	—	应	应
4.应用和数据安全	采用密码技术保证 <u>系统资源访问控制信息的完整性</u>	可	可	宜	应
5.管理制度	采用密码技术对 <u>重要可执行程序进行完整性保护</u> ，并对其来源进行真实性验证	—	—	宜	应
6.人员管理	采用密码技术保证设备中的 <u>重要信息资源安全标记完整性</u>	—	—	宜	应
7.建设运行	以上采用的 <u>密码产品</u> ，应达到GB/T 37092相应的安全要求	—	应一级以上	应二级以上	应三级以上
8.应急处置	以上如采用 <u>密码服务</u> ，该密码服务应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	应	应	应	应

应用和数据安全指标体系

	应用和数据安全-指标体系	一级	二级	三级	四级
1.物理和环境安全	采用密码技术对登录用户进行 <u>身份鉴别</u> ，保证应用系统用户身份的真实性	可	宜	应	应
2.网络和通信安全	采用密码技术保证信息系统应用的重要数据在 <u>传输过程中的机密性</u>	可	宜	应	应
	采用密码技术保证信息系统应用的重要数据在 <u>传输过程中的完整性</u>	可	宜	宜	应
3.设备和计算安全	采用密码技术保证信息系统应用的重要数据在 <u>存储过程中的机密性</u>	可	宜	应	应
	采用密码技术保证信息系统应用的重要数据在 <u>存储过程中的完整性</u>	可	宜	宜	应
4.应用和数据安全	采用密码技术保证信息系统应用的 <u>访问控制信息的完整性</u>	可	可	宜	应
5.管理制度	以上采用的 <u>密码产品</u> ，应达到GB/T 37092相应的安全要求	—	应一级以上	应二级以上	应三级以上
6.人员管理	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 <u>不可否认性</u> 和数据接收行为的不可否认性	—	—	宜	应
7.建设运行	以上如采用 <u>密码服务</u> ，该密码服务应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	应	应	应	应
8.应急处置	采用密码技术保证信息系统应用的 <u>重要信息资源安全标记完整性</u>	—	—	宜	应

管理制度指标体系

	管理制度-指标体系	一级	二级	三级	四级
1.物理和环境安全					
2.网络和通信安全	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	应	应	应	应
3.设备和计算安全	定期 对密码应用安全管理制度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	—	—	应	应
4.应用和数据安全	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	—	—	应	应
5.管理制度	具有密码应用 操作规程的相关执行记录并妥善保存	—	—	应	应
6.人员管理	根据密码应用方案建立相应 密钥管理规则	应	应	应	应
7.建设运行	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	—	应	应	应
8.应急处置					

人员管理指标体系

	人员管理-指标体系	一级	二级	三级	四级
1.物理和环境安全	相关人员应了解并遵守 <u>密码相关法律法规、密码应用安全管理制度</u>	应	应	应	应
2.网络和通信安全	<u>建立上岗人员培训制度</u> ，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	—	应	应	应
3.设备和计算安全	2级 3级 4级： <u>建立密码应用岗位责任制度</u> ，明确各岗位在安全系统中的职责和权限				
4.应用和数据安全	3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。	—	应	应	应
5.管理制度	4级： 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。				
6.人员管理	1级：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 2 3级 4级： <u>建立关键人员保密制度和调离制度</u> ，签订保密合同，承担保密义务	应	应	应	应
7.建设运行					
8.应急处置	定期对 <u>密码应用安全岗位人员进行考核</u>	—	—	应	应

建设运行指标体系

	建设运行-指标体系	一级	二级	三级	四级
1.物理和环境安全					
2.网络和通信安全	依据密码相关标准和密码应用需求， <u>制定密码应用方案</u>	应	应	应	应
3.设备和计算安全	根据密码应用方案， <u>确定系统涉及的密钥种类、体系及其生存周期环节</u> ，各环节密钥管理要求参照附录	应	应	应	应
4.应用和数据安全					
5.管理制度	按照 <u>密码应用方案实施建设</u>	应	应	应	应
6.人员管理	投入运行前进行 <u>密码应用安全性评估</u> 3级 4级：评估通过后系统方可正式运行	可	宜	应	应
7.建设运行	在运行过程中，严格执行既定的密码应用安全管理制度， <u>定期开展密码应用安全性评估及攻防对抗演习</u> ，并根据评估结果进行整改	—	—	应	应
8.应急处置					

应急处置指标体系

1.物理和环境安全	应急处置-指标体系	一级	二级	三级	四级
2.网络和通信安全	1级：根据密码产品提供的 <u>安全策略</u> ，由用户自主处置密码应用安全事件				
3.设备和计算安全	制定 <u>密码应用应急策略</u> ，做好应急资源准备，当密码应用安全事件发生时，（2级：按照应急处置措施，3级 4级：立即启动应急处置措施）结合实际情况及时处置	可	应	应	应
4.应用和数据安全					
5.管理制度	<u>事件处置</u> 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	-	-	应	应
6.人员管理					
7.建设运行	事件发生后，及时向有关信息系统主管部门（4级：及归属的密码管理部门） <u>进行报告</u>	-	-	应	应
8.应急处置					

附录：密钥生存周期管理，保证密钥全生存周期的安全性

密钥管理保证密钥(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~~应用和数据层面的~~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，并在密码应用实施中落实



密评流程

依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》编制的《信息系统密码应用测评过程指南》中提出在测评活动开展前，需要对被测信息系统的密码应用方案进行评估，通过评估的密码应用方案可以作为测评实施的依据，测评实施包括四项基本测评活动。

测评准备活动

1. 项目启动
2. 信息收集和分析
3. 测评工具和表单准备

方案编制活动

1. 确定测评对象和测评指标
2. 确定测评检查点
3. 确定测评内容
4. 编制测评方案

现场测评活动

1. 现场测评准备
2. 现场测评和结果记录
3. 结果确认和资料归还

分析与报告编制活动

1. 单项测评结果判定
2. 单元测评结果判定
3. 整体测评
4. 风险分析
5. 测评结论形成
6. 测评报告编制

信息系统密码应用高风险判定指引

范围

给出信息系统密码应用过程中可能存在的**高风险安全问题**，用于指导、规范信息系统**密码应用的规划、建设、运行及测评**。

概述

本文件中判定内容包括：

指标要求

适用范围

安全问题

可能的缓解措施

风险评价

其中，指标要求源自GB/T 39786—2021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**，在密码应用的规划、建设、运行及测

GB/T 20984、GB/T 39786—2021、GM/T 0115—2021 和 GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

关键定义

- 安全问题** security issues

资产中能被威胁所利用的弱点。

- 缓解措施** mitigation measures

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。

- 设备指纹** device fingerprinting

是指可以用于标识出该设备的设备特征或者独特的设备标识，用于区分和识别不同的设备。设备指纹因子通常包括计算机的操作系统类型、安装的各种插件、浏览器的语言设置及其时区、设备的硬件ID、手机的IMEI、电脑的网卡MAC地址等，通过某种技术措施将设备指纹因子形成特征字符串来用作设备指纹。

密码应用高风险判定 - 以某企业办公楼一层机房为例说明

1.通用要求

密码算法

- 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。
- 适用范围：所有级别信息系统。
- 安全问题：**使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；使用安全性未知的密码算法，如自行设计的密码算法、未经安全性论证的密码算法等。
- 可能的缓解措施：无。
- 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

密码技术

- 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。
- 适用范围：所有级别信息系统。
- 安全问题：**使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；使用安全性未知的密码技术，如自行设计的密码通信协议、未经安全性论证的密码通信协议等。
- 可能的缓解措施：无。
- 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

密码产品和密码服务

- 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。
- 适用范围：所有级别信息系统。
- 安全问题：**使用自实现且未提供安全性证据的密码产品；使用的密码产品存在高危安全漏洞，如存在Heartbleed漏洞的OpenSSL；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；使用的密码服务，其密码服务提供者不具有相关资质；存在可能会对密钥管理造成严重安全隐患的安全问题（见附录A）。
- 可能的缓解措施：无。
- 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

注：

业务

运维



2.物理和环境安全

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A

密钥管理

安全问题

物理和环境安全 - 身份鉴别

1.通用要求

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。

适用范围：第二级及以上级别信息系统。

安全问题：

- ① 存在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 人员身份真实性的密码技术实现机制不正确或无效。

可能的缓解措施：

- ① 基于生物识别技术（如指纹等）对重要区域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



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

2.物理和环境安全

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题

网络和通信安全 - 身份鉴别

1.通用要求

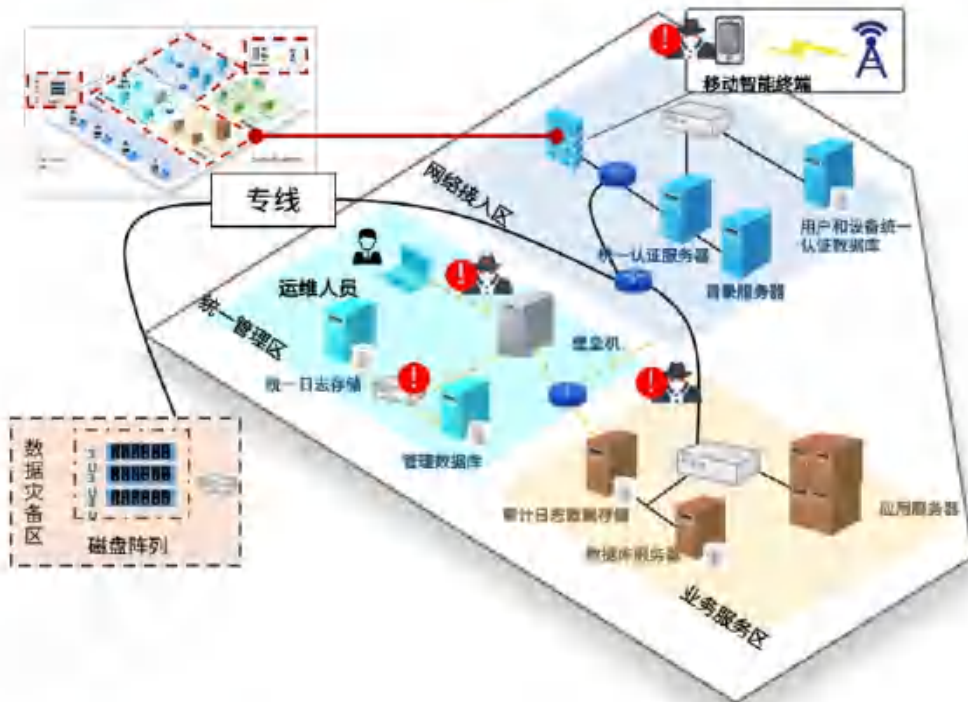
指标要求：采用密码技术对通信实体进行身份鉴别（第三级）/双向身份鉴别（第四级），保证通信实体身份的真实性。

适用范围：第三级及以上级别信息系统。

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通信实体进行身份鉴别；
- ③ 通信实体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）。

可能的缓解措施：无



风险评价：

上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

2.物理和环境安全

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题

网络和通信安全 - 通信过程中重要数据的机密性

1.通用要求

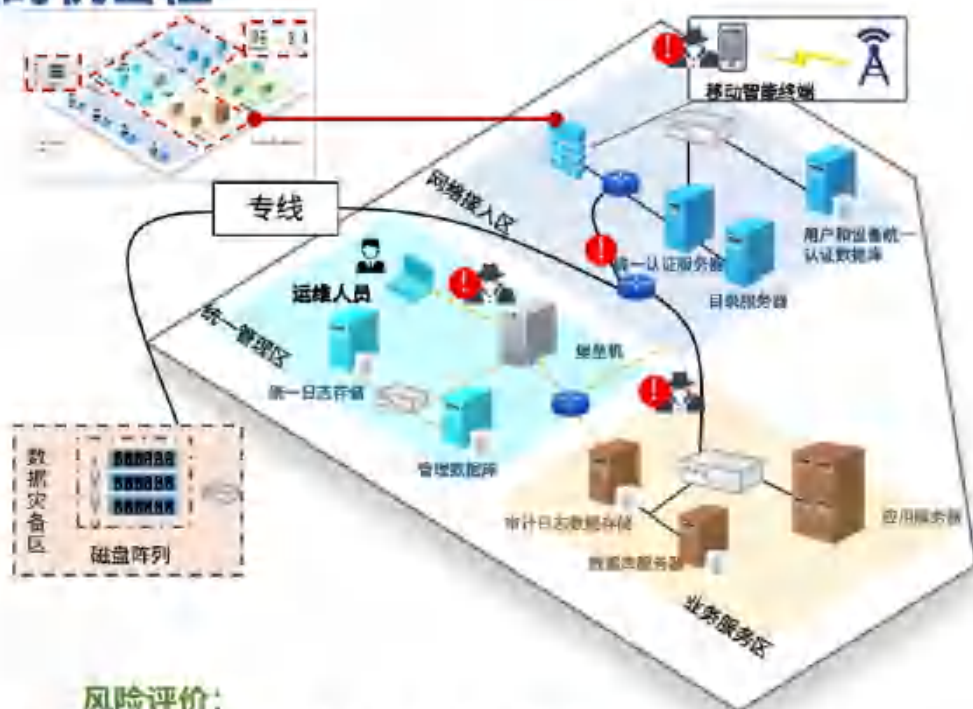
指标要求：采用密码技术保证通信过程中重要数据的机密性。

适用范围：第三级及以上级别信息系统。

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通信过程中重要数据进行机密性保护；
- ③ 通信过程中重要数据机密性保护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）。

可能的缓解措施：在“应用和数据安全”层面针对信息系统所有需要保护的重要数据传输采用符合要求的密码技术进行机密性保护，且加密后的数据流能够覆盖网络通信信道。



风险评价：

若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，或重要数据机密性保护的密码技术实现机制不正确或无效，但在“应用和数据安全”层面针对信息系统所有需要保护的重要数据传输采用符合要求的密码技术进行机密性保护，且加密后的数据流能够覆盖网络通信信道，可酌情降低风险等级。

2.物理和环境安全

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A

密钥管理安全问题

网络和通信安全 - 安全接入认证

1.通用要求

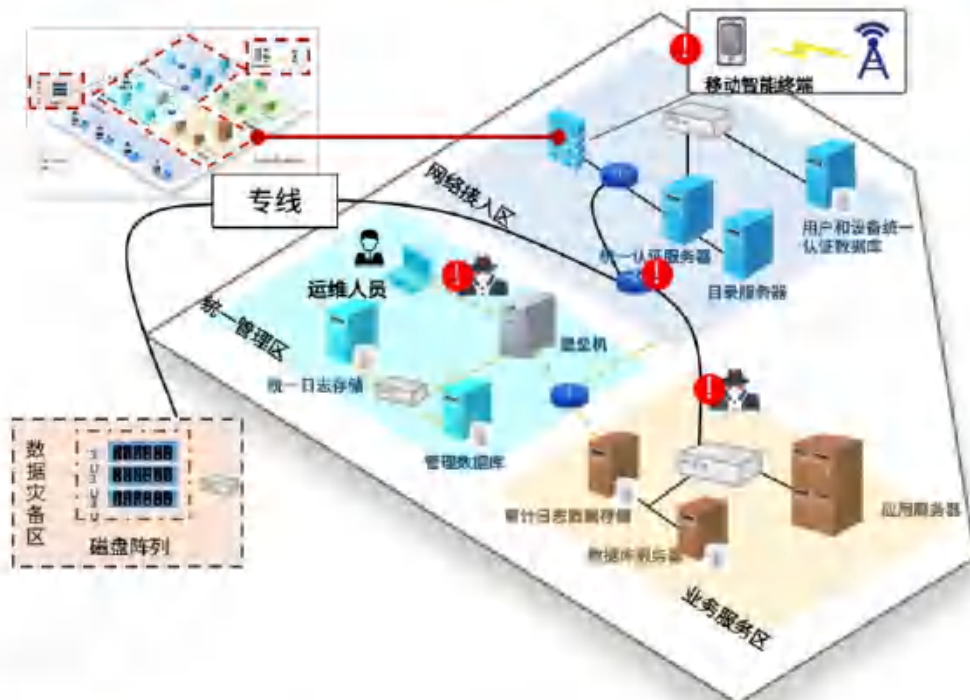
指标要求：采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。

适用范围：第四级及以上级别信息系统。

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）。

可能的缓解措施：无。



风险评价：

上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

2.物理和环境安全

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题

设备和计算安全 - 身份鉴别

1.通用要求

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。

适用范围：第三级及以上级别信息系统。

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。

可能的缓解措施：基于特定识别技术（如设备指纹、生物指纹等）保证用户身份的真实性。



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**基于特定识别技术**（如设备指纹、生物指纹等）保证用户身份的真实性，可酌情降低风险等级。

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题

设备和计算安全 - 远程管理通道安全

1.通用要求

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。

2.物理和环境安全

适用范围：第三级及以上级别信息系统。

3.网络和通信安全

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的密码技术实现机制**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。

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题

可能的缓解措施：搭建了与业务网络物理隔离、采取相应的安全防护措施的专用管理网络（如带外管理网络）进行远程管理；在“网络和通信安全”层面使用SSL VPN网关、IPSec VPN网关等相关设备建立专用的集中管理通道，且采用的密码技术符合要求。



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的密码技术实现机制不正确或无效，但通过搭建与业务网络物理隔离、采取相应的安全防护措施的专用管理网络进行远程管理，可酌情降低风险等级；
- ② 若在“网络和通信安全”层面使用SSL VPN网关、IPSec VPN网关等相关设备建立专用的集中管理通道，且采用的密码技术符合要求，可酌情

应用和数据安全 - 身份鉴别

1.通用要求

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。

2.物理和环境安全

适用范围：第三级及以上级别信息系统。

3.网络和通信安全

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）。

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题

可能的缓解措施：基于特定识别技术（如设备指纹、生物指纹、第三方身份鉴别服务等）保证用户身份的真实性。



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，基于特定识别技术（如设备指纹、生物指纹、第三方身份鉴别服务等）保证用户身份的真实性，可酌情降低风险等级。

应用和数据安全 - 重要数据传输机密性

1.通用要求

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。

适用范围：第三级及以上级别信息系统。

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保护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）。

可能的缓解措施：在“网络和通信安全”层面通信实体间采用符合要求的密码技术建立网络通信信道，且网络通信信道经评估无高风险。

2.物理和环境安全

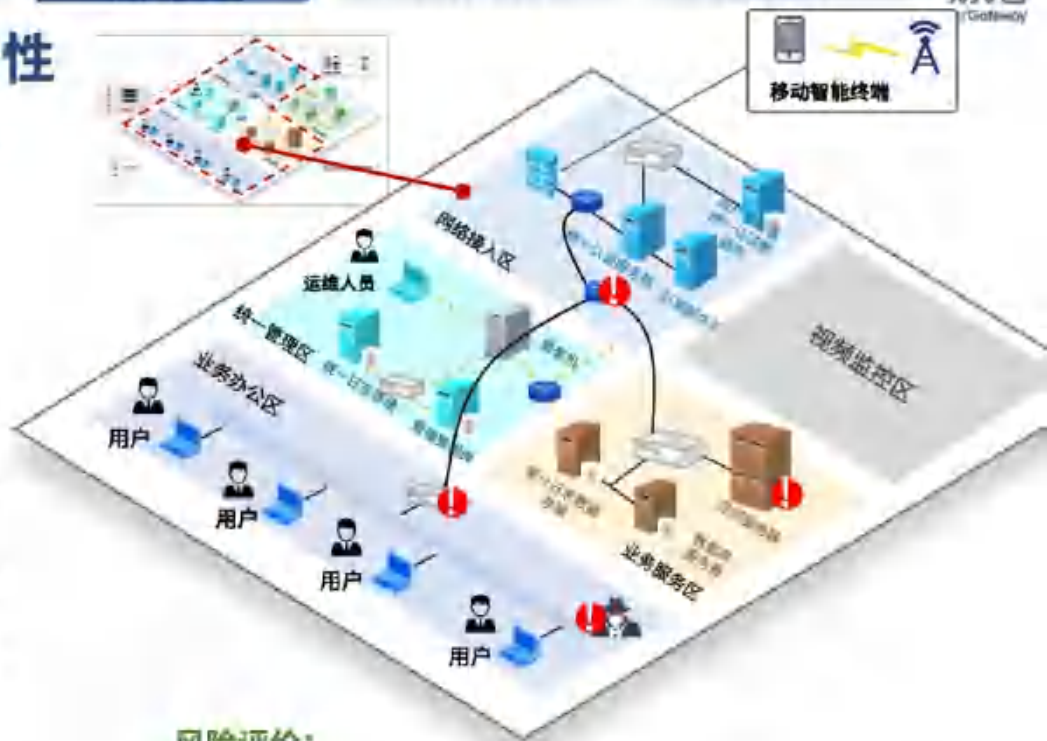
3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题



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，或重要数据传输机密性保护的实现机制不正确或无效，但在“网络和通信安全”层面通信实体间采用符合要求的密码技术建立网络通信信道，且网络通信信道经评估无高风险，可酌情降低风险等级。

应用和数据安全 - 重要数据存储机密性

1.通用要求

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。

适用范围：第三级及以上级别信息系统。

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保护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）。

可能的缓解措施：无。

2.物理和环境安全

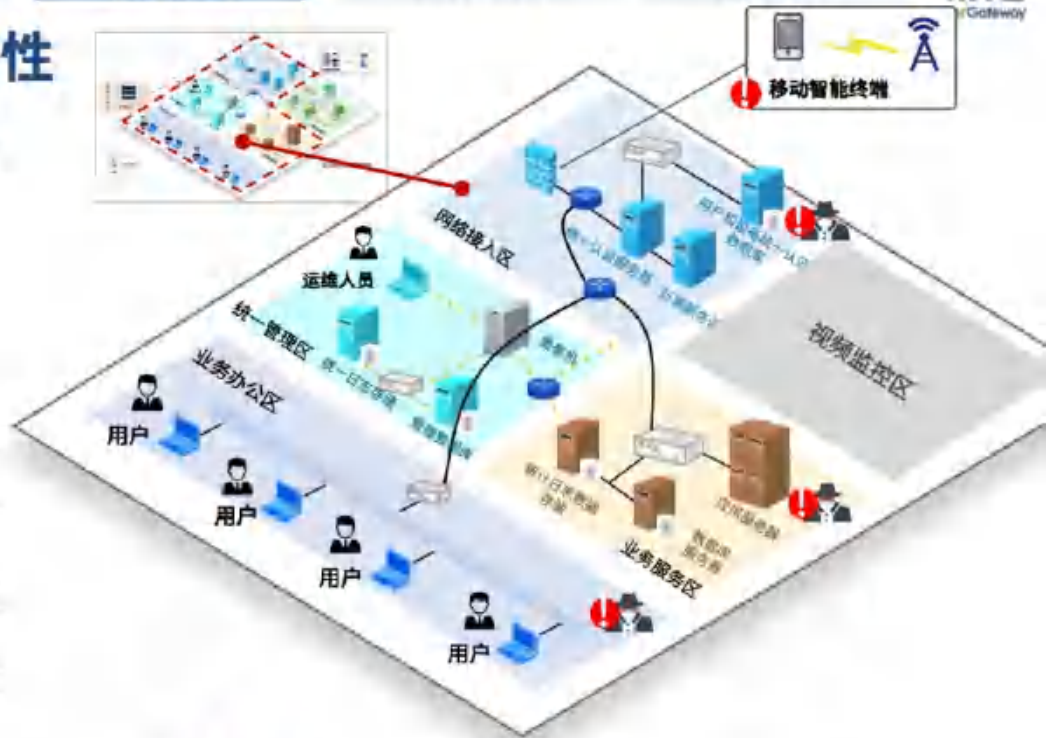
3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A 密钥管理 安全问题



风险评价：

上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

应用和数据安全 - 重要数据存储完整性

1.通用要求

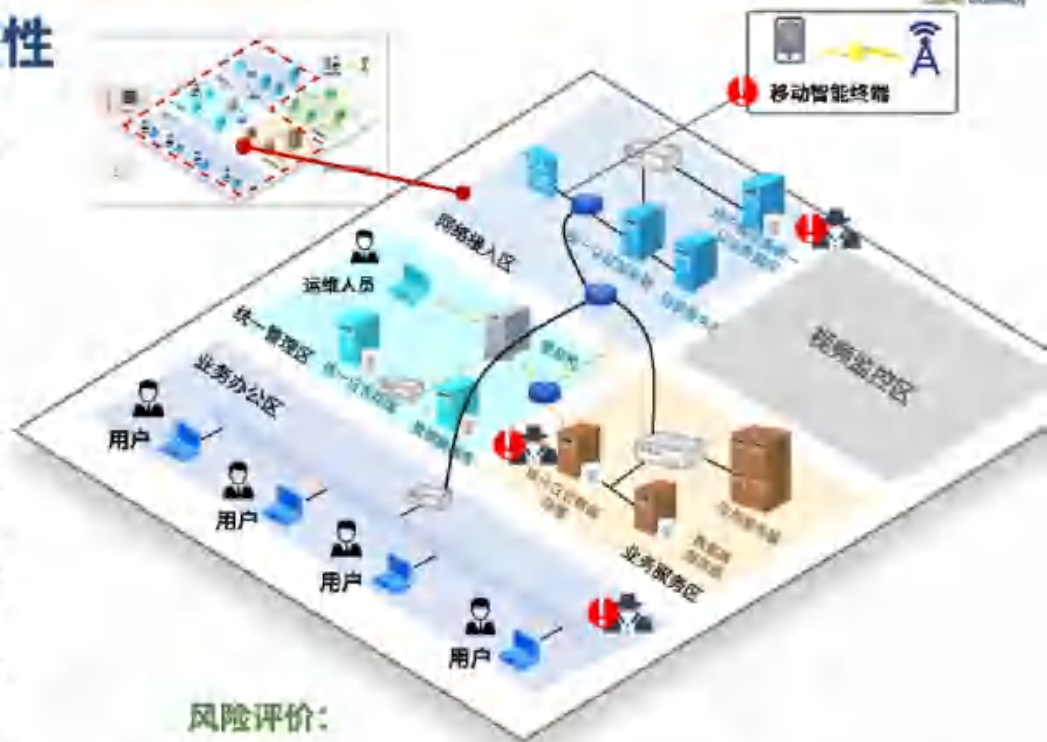
指标要求：采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。

适用范围：第三级及以上级别信息系统。

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保护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）。

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。



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保护的密码技术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

附录A
密钥管理
安全问题

应用和数据安全 - 不可否认性

1.通用要求

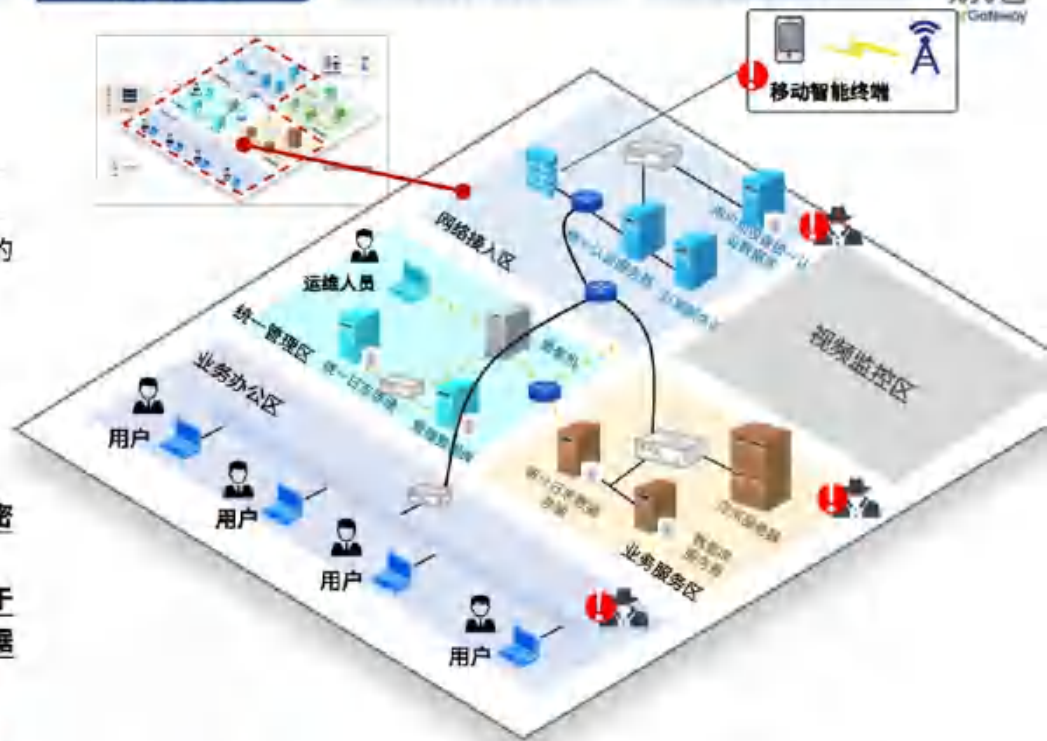
指标要求：在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

适用范围：第三级及以上级别信息系统。

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）。

可能的缓解措施：无。



风险评价：

上述任一安全问题一旦被威胁利用后，可能会导致信息系统面临高风险。

2.物理和环境安全

3.网络和通信安全

4.设备和计算安全

5.应用和数据安全

6.密码应用管理要求

附录A

密钥管理安全问题

密码应用管理要求

1.通用
要求

2.物理和
环境安全

3.网络和
通信安全

4.设备和
计算安全

5.应用和
数据安全

6.密码应
用管理要
求

附录A
密钥管理
安全问题

具备密码应用安全管理制度

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。

适用范围：第二级及以上级别信息系统。

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。

可能的缓解措施：无

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风险。

制定密码应用方案

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。

适用范围：第二级及以上级别信息系统。

安全问题：

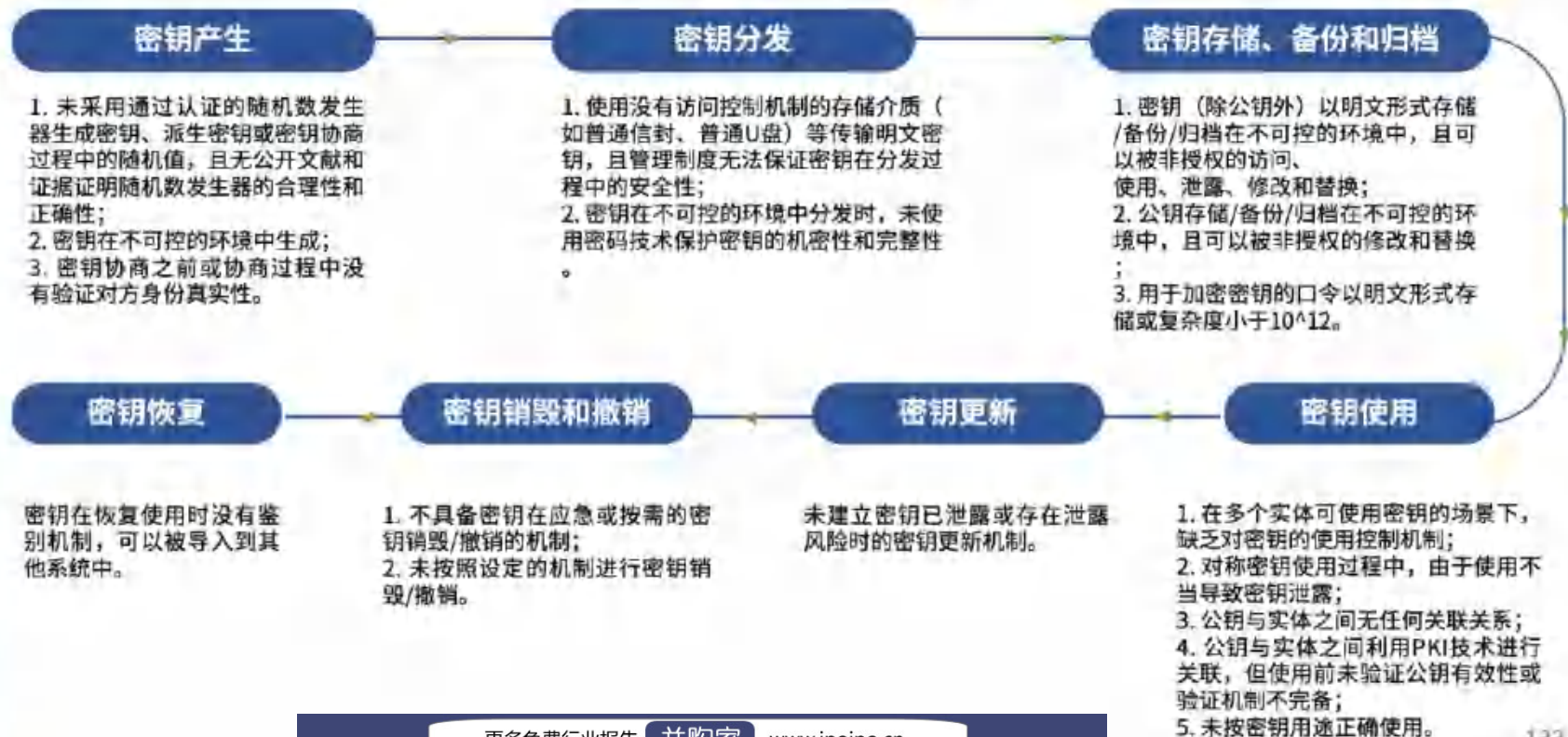
信息系统未制定密码应用方案或密码应用方案未通过评审。

可能的缓解措施：如被测系统通过测评发现不存在高风险安全问题，可酌情降低风险等级。

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。密钥管理各环节，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：



商用密码应用安全性评估量化评估规则

《信息安全技术信息系统密码应用基本要求》

GB/T 39786-2021

《信息系统密码应用测评要求》

GM/T0115-2021

制定依据

商用密码应用安全性评估量化评估规则（2023版）

指导、规范信息系统密码应用的规划、建设、运行及测评

设计原则

- ① 遵循法律法规和最新相关指导性文件的总体要求；
- ② 遵循 GB/T 39786-2021 和 GM/T 0115-2021；
- ③ **鼓励使用密码技术；特别鼓励使用合规的密码算法/技术/产品/服务；**
- ④ 优先在网络和通信安全层面、应用和数据安全层面推进密码技术应用。

量化评估框架

密码使用有效性

Cryptography Deployment Effectiveness

密码技术是否被正确、有效使用，以满足信息系统的安全需求，有效提供机密性、完整性、真实性和不可否认性的保护；

密码算法/技术合规性

Cryptography Algorithm/Technique Compliance

信息系统中使用密码算法是否符合法律、法规规定和密码相关国家标准、行业标准的有关要求，信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准或经国家密码管理部门核准。

密钥管理安全

Key Management Security

密钥管理的全生命周期是否安全，用于密码计算或密钥管理的密码产品/密码服务是否安全。

量化规则和整体结论判定

各测评对象的测评结果量化评估规则

密码应用技术要求中，第 i 个安全层面的第 j 测评单元的第 k 测评对象 $T_{i,j,k}$ ，其量化评估结果 $S_{i,j,k} \in \{0, 0.25, 0.5, 1\}$

其中，0表示不符合，其它表示部分符合，1表示符合。 $S_{i,j,k}$ 的取值分别见表 1。

通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标不单独评价。密码应用管理要求不针对各个测评对象的测评结果进行量化评估。

测评单元的测评结果量化评估规则

密码应用技术要求中，第 i 个安全层面的第 j 测评单元 $U_{i,j}$ 的量化评估结果 $S_{i,j}$ 为该测评单元内所有 $n_{i,j}$ 个测评对象测评结果的算术平均值（四舍五入，取小数点后 4 位），即：

$$S_{i,j} = \frac{\sum_{1 \leq k \leq n_{i,j}} S_{i,j,k}}{n_{i,j}}$$

密码应用管理要求中，第 i 个安全层面的第 j 测评单元，根据 GM/T 0115-2021 给出判定结果 $S_{i,j}$ ，不符合为 0 分，部分符合为 0.5 分，符合为 1 分。

安全层面的测评结果量化评估规则

本文件为每个测评单元分配了相应的权重 $w_{i,j}$ ，如表 2 所示。第 i 个安全层面 L_i 的量化评估结果 S_i 为该安全层面内所有 n_i 个适用测评单元测评结果 $S_{i,j}$ 的加权平均值（四舍五入，取小数点后 4 位）

$$S_i = \frac{\sum_{1 \leq j \leq n_i} w_{i,j} S_{i,j}}{\sum_{1 \leq j \leq n_i} w_{i,j}}$$

若某测评指标不适用，则不参与量化评估过程，不适用的判定方式参见 GM/T 0115-2021。

整体测评结果量化评估规则

本文件为每个安全层面分配了相应的权重 w_i ，如表 2 所示。量化评估结果 S 为所有 n 个安全层面测评结果 S_i 的加权平均值（四舍五入，取小数点后 2 位），即：

$$S = \frac{\sum_{1 \leq i \leq n} w_i \cdot S_i}{\sum_{1 \leq i \leq n} w_i} \times 100$$

若某个安全层面的所有测评指标都不适用，则该安全层面不参与量化评估过程。如，信息系统中“物理和环境安全”层面所有测评指标都不适用，而其他各层面均有适用的测评指标，根据表 2 提供的安全层面权重，上述分值计算公式为：

$$S = \frac{\sum_{1 \leq i \leq n} w_i \cdot S_i}{\sum_{1 \leq i \leq n} w_i} \times 100 = \frac{\sum_{1 \leq i \leq n} w_i \cdot S_i}{40} \times 100$$

整体结论判定

- 整体量化评估结果 **S 为 100 分**，则判定被测信息系统符合 GB/T 39786-2021 相应等级要求；
- S 低于 100 分、不低于阈值**，且经风险评估发现没有高风险，则判定被测信息系统基本符合 GB/T 39786-2021 相应等级要求；
- 否则，判定被测信息系统不符合 GB/T 39786-2021 相应等级要求。

量化评估表1

符合情况	涉及情况			示例	分值 $S_{i,j,k}$
	密码使用安全 D	密码算法/技术合规性 A	密钥管理安全 K		
符合	√	√	√	全部符合相关的要求	1
部分符合	√	×	√	使用认证合格的密码产品，但使用的密码算法/技术不合规	0.5
	√	√	×	使用未经认证或不满足安全等级要求的密码产品，但使用的密码算法/技术合规	
	√	×	×	使用未经认证或不满足安全等级要求的密码产品，且使用的密码算法/技术不合规	0.25
不符合	×	/	/	使用的密码技术无法满足信息系统的安全需求，或未使用密码技术等	0

测评指标权重表2

要求 维度	安全层 面序号 i	安全 层面	测评单 元序号 j	测评单元	安全层面 权重 (w_i)	指标权重 w_{ij}			
						第一级	第二级	第三级	第四级
密码 技术 应用 要求	1	物理和 环境安 全	(1)	身份鉴别	10	0.4	0.7	1	1
			(2)	电子门禁记录数据存储完整性		0.4	0.4	0.7	1
			(3)	视频记录数据存储完整性		/	/	0.7	1
	2	网络和 通信安 全	(1)	身份鉴别	20	0.4	0.7	1	1
			(2)	通信数据完整性		0.4	0.4	0.7	1
			(3)	通信过程中重要数据的机密性		0.4	0.7	1	1
			(4)	网络边界访问控制信息的完整性		0.4	0.4	0.7	1
			(5)	安全接入认证		/	/	0.4	0.7
	3	设备和 计算安 全	(1)	身份鉴别	10	0.4	0.7	1	1
			(2)	远程管理通道安全		/	/	1	1
			(3)	系统资源访问控制信息完整性		0.4	0.4	0.7	1
			(4)	重要信息资源安全标记完整性		/	/	0.7	1
			(5)	日志记录完整性		0.4	0.4	0.7	1
			(6)	重要可执行程序完整性、重要可执行程序来源真实性		/	/	0.7	1

测评指标权重表2

要求 维度	安全层 面序号 i	安全 层面	测评单 元序号 j	测评单元	安全层面权 重 (w _i)	指标权重w _{i,j}			
						第一级	第二级	第三级	第四级
密码 技术 应用 要求	4	应用和 数据安 全	(1)	身份鉴别	30	0.4	0.7	1	1
			(2)	访问控制信息完整性		0.4	0.4	0.7	1
			(3)	重要信息资源安全标记完整性			/	0.7	1
			(4)	重要数据传输机密性		0.4		0.7	1
			(5)	重要数据存储机密性		0.4	0.7	1	1
			(6)	重要数据传输完整性		0.4	0.7	1	1
			(7)	重要数据存储完整性		0.4	0.7	1	1
			(8)	不可否认性		/	/	1	1
			安全 管理	5		管理 制度	(1)	具备密码应用安全管理制度	8
(2)	密钥管理规则	0.7			0.7		0.7	0.7	
(3)	建立操作规程	/			0.7		0.7	0.7	
(4)	定期修订安全管理制度	/			/		0.7	0.7	
(5)	明确管理制度发布流程	/			/		0.7	0.7	
(6)	制度执行过程记录留存	/			/		0.7	0.7	

测评指标权重表2

要求 维度	安全层 面序号j	安全层面	测评单 元序号 j	测评单元	安全层 面权重 (wi)	指标权重wi,j			
						第一 级	第二 级	第三 级	第四 级
安全管理	6	人员管理	(1)	了解并遵守密码相关法律法规和密码管理制度	8	0.7	0.7	0.7	0.7
			(2)	建立密码应用岗位责任制度		/	1	1	1
			(3)	建立上岗人员培训制度		/	0.7	0.7	0.7
			(4)	定期进行安全岗位人员考核		/	/	0.7	0.7
			(5)	建立关键岗位人员保密制度和调离制度		0.7	0.7	0.7	0.7
	7	建设运行	(1)	制定密码应用方案	8	1	1	1	1
			(2)	制定密钥安全管理策略		1	1	1	1
			(3)	制定实施方案		0.7	0.7	0.7	0.7
			(4)	投入运行前进行密码应用安全性评估		1	1	1	1
			(5)	定期开展密码应用安全性评估及攻防对抗演习		/	/	0.7	0.7
	8	应急处置	(1)	应急策略	6	1	1	1	1
			(2)	事件处置		/	/	0.7	0.7
			(3)	向有关主管部门上报处置情况		/	/	0.7	0.7

测评结论

方案评估结论

通过 或 不通过

方案评估结论格式如下：

受{委托单位}委托，{密评机构名称}于XX年XX月XX日至XX年XX月XX日，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GM/T 0115—2021《信息系统密码应用测评要求》的第XX{（一～四）}级相关要求，对《XX系统密码应用方案》进行了商用密码应用安全性评估，结论为：
{通过/不通过}。

系统测评结论

量化评估结果S为所有n个安全层面测评结果的加权平均值（四舍五入，取小数点后2位）。依据量化评估结果S的分值来判断系统评测结果：符合、基本符合、不符合。

- **符合**：整体量化评估结果**S为100分**，则判定被测信息系统符合GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》相应等级要求；
- **基本符合**：**S低于100分、不低于阈值**，且经风险评估发现没有高风险，则判定被测信息系统基本符合GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》相应等级要求；
- **不符合**：否则，判定被测信息系统**不符合**GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》相应等级要求。

更新解读

01 密评背景介绍

02 密评总体要求

03 密评测评要求

04 密评方案要求

05 密评测评过程

06 密评团标解读

07 密改FAQ解读

08 密改方案实践



GB/T43206-2023 信息安全技术 信息系统密码应用测评要求

2023年9月7日，国家标准化管理委员会发布GB/T43206-2023 信息安全技术 信息系统密码应用测评要求，并于2024年4月1日起实施。该国标有助于提高信息系统密码应用的安全性和可靠性，成为今后密码测评工作的重要抓手。



明确五大术语和定义

GB/T 25069-2022、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。



密码应用安全性 评估人员

通过国家密码管理部门认可的考核或具有密码技术应用员、密码工程技术人員职业技能等级证书，从事密码应用安全性评估的人员。

注：简称“密评人员”



核查

密评人员对测评对象进行访谈、文档审查、实地查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

注：核查时可选用的测评方式以及方式的选用说明参考 GM/T 0116-2021



测评单元

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。



测评指标

测评单元中第一级到第四级密码应用测评的具体要求。



测评对象

测评单元中密码应用的测评实施对象。

注：主要包括物理安防设施、通信信道、密码产品、通用设备、应用、重要数据、人员、制度文档等。测评对象基于密码应用方案和信息系統保护目标的实际安全需求确定，具体确定方法参考 GM/T 0116-2021。

国标通则：对信息系统密码应用等级测评指标以“应”“宜”“可”进行描述

密评人员在开展实际测评时，按照如下方法确定是否纳入测评和结果判定范围。



特殊情况

如信息系统通过评估的密码应用方案要求高于其自身对应等级的测评指标要求，则密评人员应按照密码应用方案要求进行测评。

例如

密码应用方案要求第三级的信息系统部分指标按照第四级进行规划、建设、运行，则对应指标按照密码应用等级第四级进行测评，并在密码应

通用测评要求涵盖密码算法、技术、产品、服务及密钥管理

通用测评要求	测评单元 通用测评项	测评指标	测评对象	测评实施
6.技术测评要求	密码算法	信息系统中使用的密码算法符合法律、法规的规定和密码相关国家标准、行业标准的有关要求(适用于第一级到第四级)。	信息系统中使用的密码算法。	了解信息系统中使用的密码算法的名称、用途、何处使用、执行设备及其实现方式(软件、硬件或固件),核查信息系统中使用的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。
7.管理测评要求	密码技术	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(适用于第一级到第四级)。	信息系统中使用的密码技术。	了解信息系统中使用的密码技术的名称、用途、何处使用、执行设备及其实现方式(软件、硬件或固件),核查信息系统中使用的密码技术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。
8.整体测评要求	密码产品	本单元测评指标如下。 信息系统中使用的密码产品符合法律法规和密码相关国家标准、行业标准的相关要求(适用于第一级到第四级)。 信息系统中使用的密码产品如遵循密码模块相关标准,则应: ——达到密码模块安全等级一级及以上安全要求(适用于第二级); ——达到密码模块安全等级二级及以上安全要求(适用于第三级); ——达到密码模块安全等级三级及以上安全要求(适用于第四级)。	信息系统中使用的密码产品。	了解信息系统中使用的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,例如其安全策略或使用手册说明的部署条件。遵循了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。
9.风险分析和评价	密码服务	信息系统中使用的密码服务符合法律法规的相关要求(适用于第一级到第四级)。	信息系统中使用的密码服务。	核查信息系统中使用的密码服务是否符合法律法规的相关要求。
10.测评结论	密钥管理	本单元测评指标如下: ——信息系统中密钥管理使用的密码产品、密码服务符合法律法规和密码相关国家标准、行业标准的要求(适用于第一级到第四级); ——信息系统中密钥管理应符合密码相关国家标准和行业标准的要求(适用于第一级到第四级)。	信息系统中密钥管理使用的密码产品、密码服务以及密钥管理实现。	本单元测评实施如下: a) 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; b) 核查信息系统中密钥管理实现是否安全、正确、有效。例如:非公开密钥是否能被非授权访问、使用、泄露、修改和替换,公开密钥是否能被非授权修改、使用。详细测评实施要点可见附录 A。
附录	更多免费行业报告 并购买家 www.ipoiipo.cn			

密码应用测评要求 - 以某企业办公楼一层机房为例说明

5.通用测评要求

6.技术测评要求

7.管理测评要求

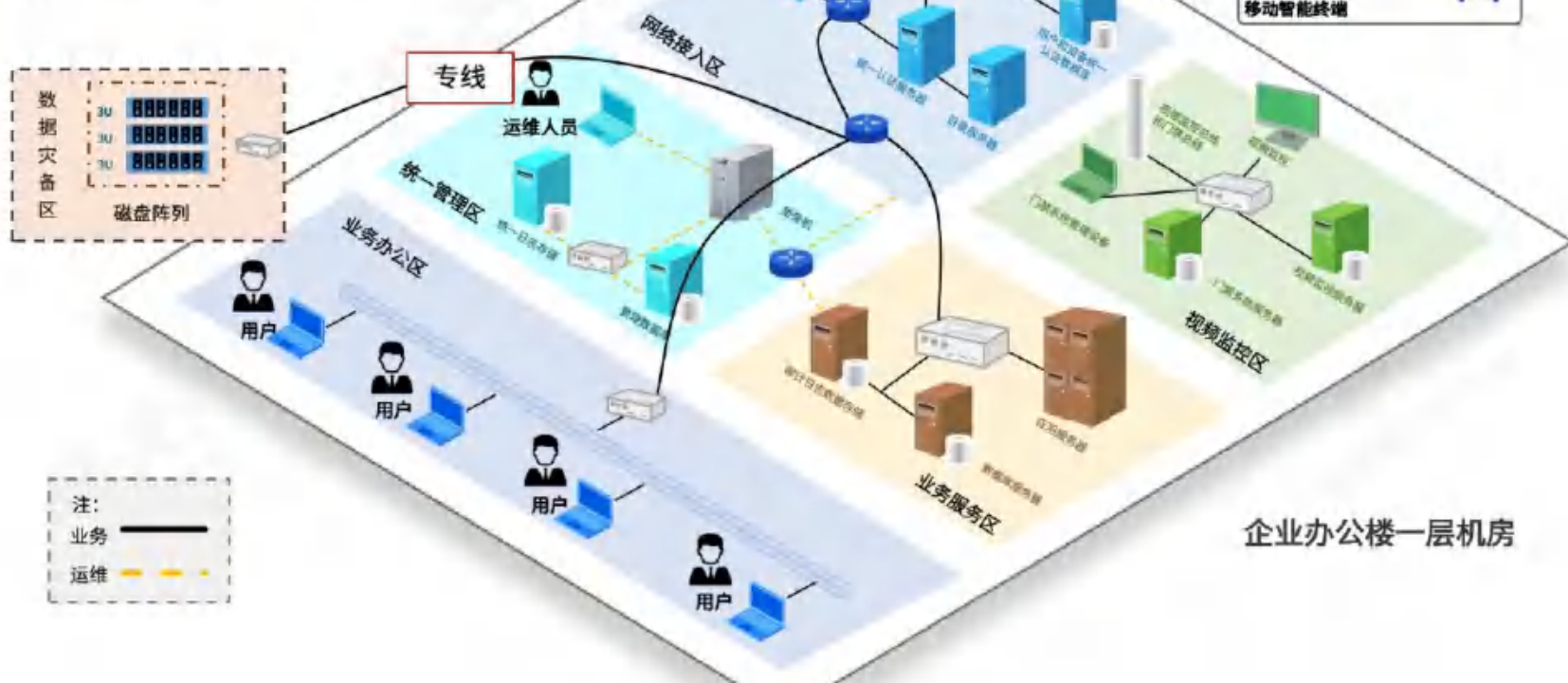
8.整体测评要求

9.风险分析和评价

10.测评结论

附录

系统部署在企业局域网，主要服务于内部工作人员，为企业内部业务专网，未与其他系统互联。用户可通过部署在业务办公区的 PC 终端浏览器访问登录，也可在互联网通过移动终端访问登录。



物理和环境安全 - 身份鉴别

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则**符合**
- 如果❌为否，则**不符合**
- 其他情况，则为**部分符合**

- 汇总判定结果均为符合，则**符合**
- 汇总判定结果均为不符合，则**不符合**



测评指标

可采用密码技术进行**物理访问身份鉴别**，保证重要区域进入人员身份的真实性(适用于**第一级**)；
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(适用于**第二级到第三级**)；
应采用密码技术进行**物理访问身份鉴别**，保证重要区域进入人员身份的真实性(适用于**第四级**)。



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。



测评实施

- 核查是否符合**密码算法** (5.1)、**密码技术** (5.2) 的要求。
- 核查是否符合**密码产品** (5.3)、**密码服务** (5.4)、**密钥管理** (5.5) 的要求。
- 核查**电子门禁系统**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。

物理和环境安全 - 电子门禁记录数据存储完整性



测评指标

可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(适用于第一级到第二级);
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(适用于第三级);
应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(适用于第四级)。



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。



测评实施

- 1 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 2 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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。

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则符合
- 如果 否 为否，则不符合
- 其他情况，则为部分符合
- 汇总判定结果均为符合，则符合
- 汇总判定结果均为不符合，则不符合

物理和环境安全 - 视频监控记录数据存储完整性

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则**符合**
- 如果★为否，则**不符合**
- 其他情况，则为**部分符合**
- 汇总判定结果均为**符合**，则**符合**
- 汇总判定结果均为**不符合**，则**不符合**



测评指标

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(适用于第三级);

应采用密码技术保证视频监控音像记录数据的存储完整性(适用于第四级)



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。



测评实施



核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。



核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。



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。

网络和通信安全 - 身份鉴别

5.通用测评要求

6.技术测评要求

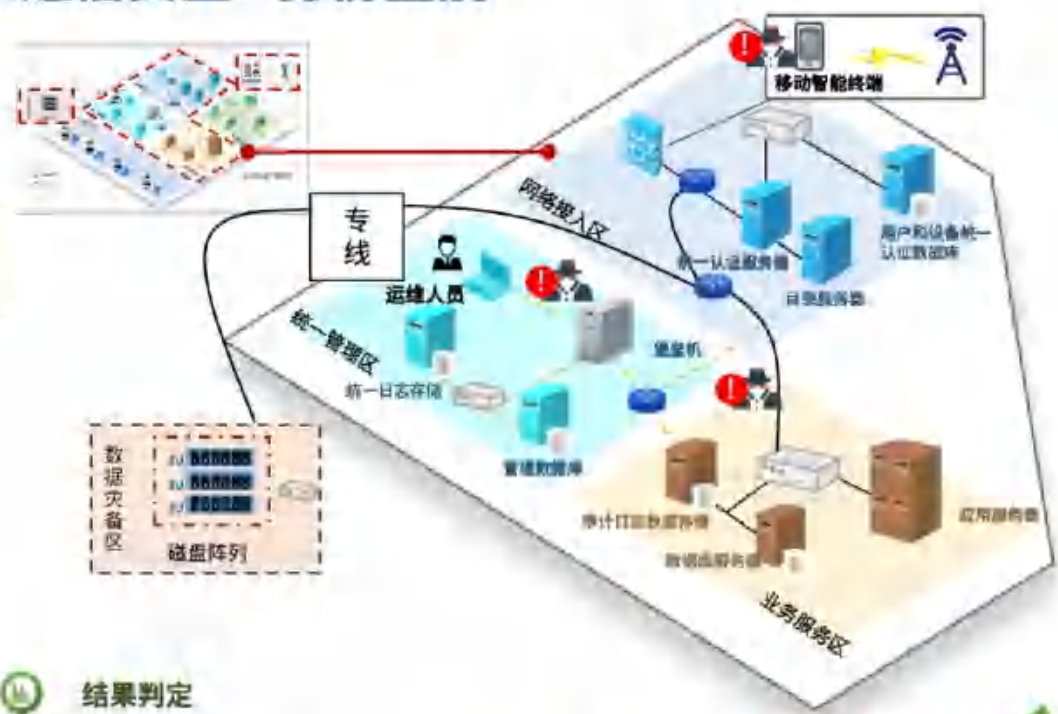
7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元如涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则符合
- 如果否，则不符合
- 其他情况，则为部分符合
- 汇总判定结果均为符合，则符合
- 汇总判定结果均为不符合，则不符合

测评指标

- 可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(适用于第一级)；
- 宜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(适用于第二级)；
- 应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(适用于第三级)；
- 应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(适用于第四级)。

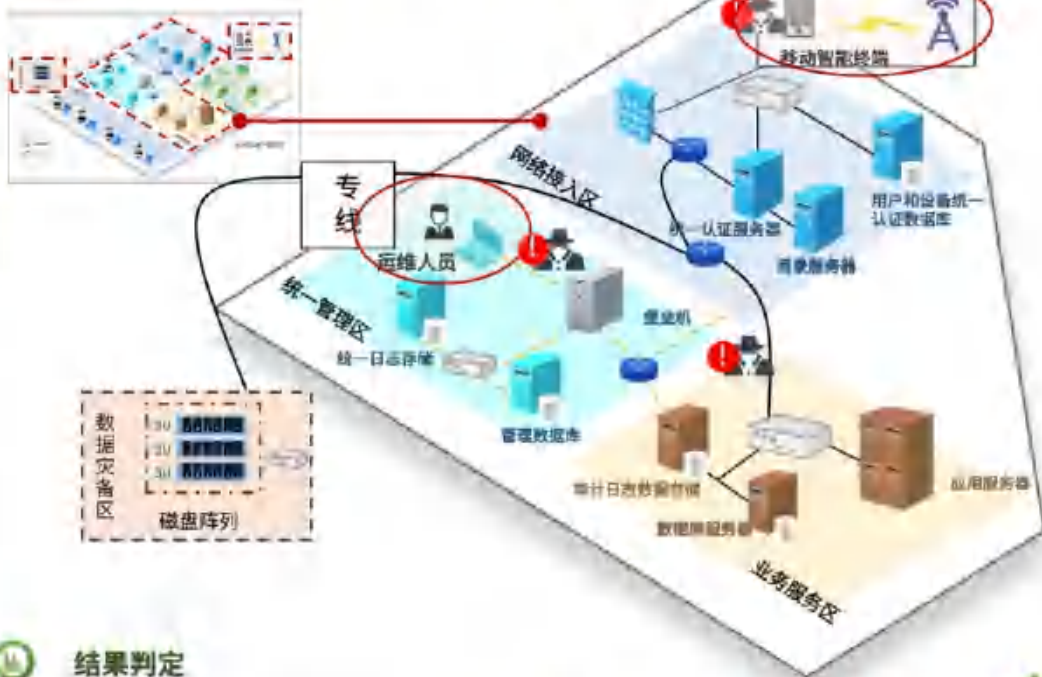
测评对象

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设备或组件、密码产品等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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(适用于第一级到第三级)/双向身份鉴别(适用于第四级)并验证通信实体身份真实性实现机制是否正确有效。

网络和通信安全 - 通信数据完整性



测评指标

可采用密码技术保证通信过程中数据的完整性(适用于第一级到第二级);
宜采用密码技术保证通信过程中数据的完整性(适用于第三级);
应采用密码技术保证通信过程中数据的完整性(适用于第四级)。

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设备或组件、密码产品等。

测评实施

★ 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。

★ 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。

★ 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。

结果判定

单个测评对象

- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则**符合**
- 如果★为否, 则**不符合**
- 其他情况, 则为**部分符合**
- 汇总判定结果均为**符合**, 则**符合**
- 汇总判定结果均为**不符合**, 则**不符合**

网络和通信安全 - 通信过程中重要数据的机密性

5.通用测评要求

6.技术测评要求

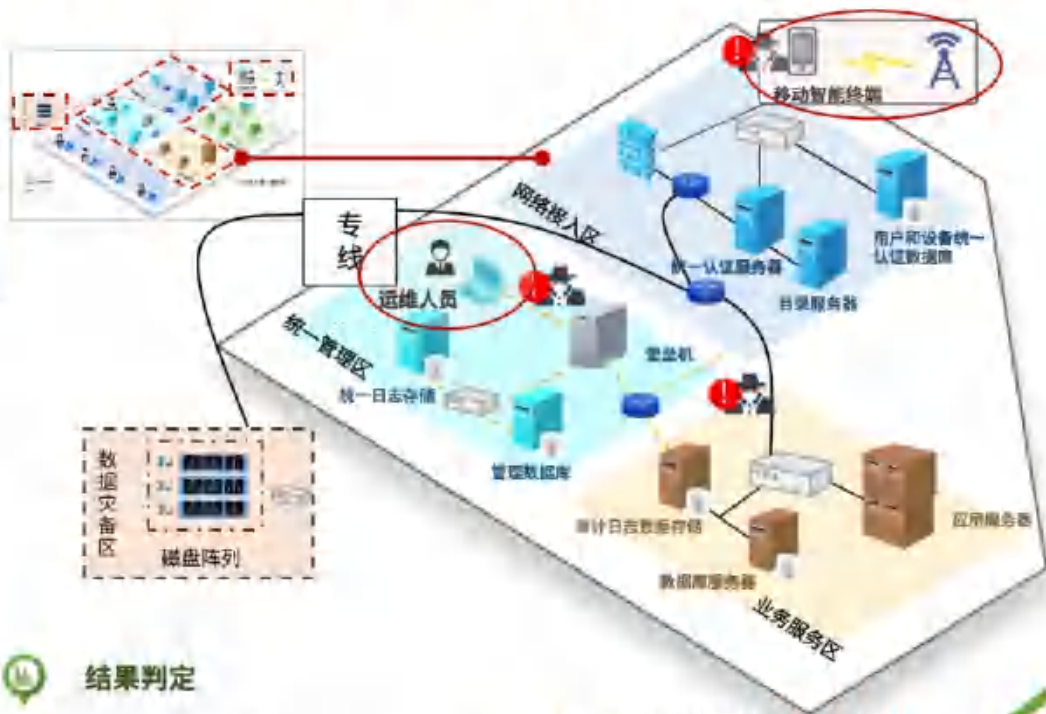
7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



测评指标

可采用密码技术保证通信过程中重要数据的机密性(适用于第一级);
宜采用密码技术保证通信过程中重要数据的机密性(适用于第二级);
应采用密码技术保证通信过程中重要数据的机密性(适用于第三级到第四级)。



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设备或组件、密码产品。



测评实施

- 1 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 2 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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。

结果判定

单个测评对象

- 本单元如涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则符合
- 如果  为否, 则不符合
- 其他情况, 则为部分符合
- 汇总判定结果均为符合, 则符合
- 汇总判定结果均为不符合, 则不符合

网络和通信安全 - 网络边界访问控制信息的完整性

5.通用测评要求

6.技术测评要求

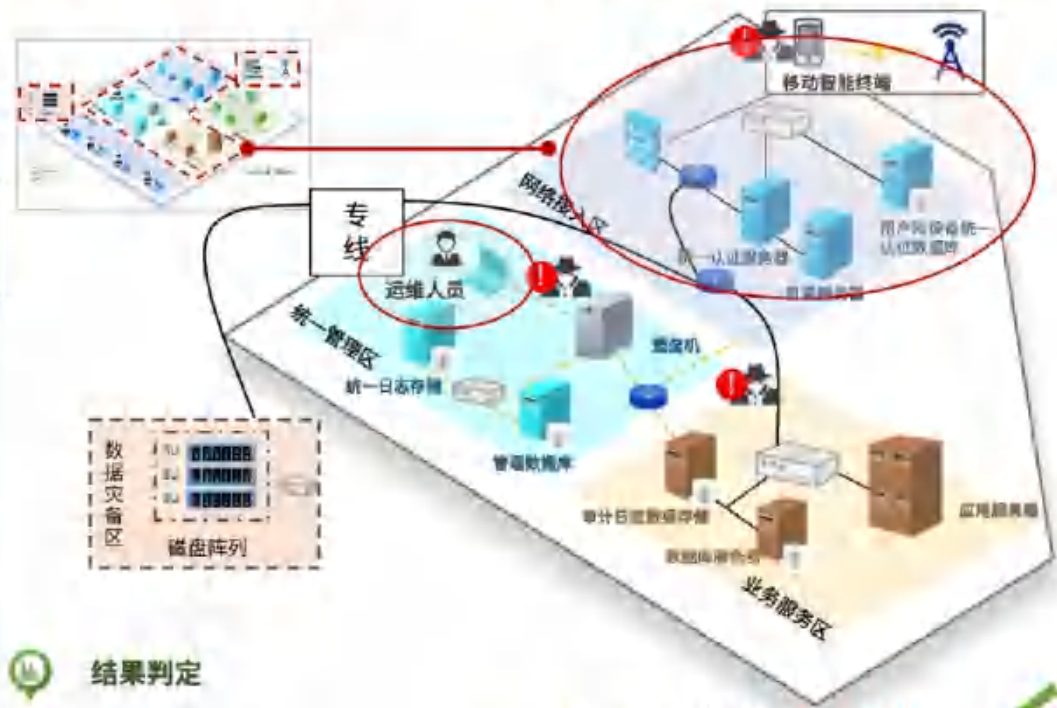
7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元如涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则符合
- 如果否，则不符合
- 其他情况，则为部分符合
- 汇总判定结果均为符合，则符合
- 汇总判定结果均为不符合，则不符合

测评指标

- 可采用密码技术保证网络边界访问控制信息的完整性(适用于第一级到第二级);
- 宜采用密码技术保证网络边界访问控制信息的完整性(适用于第三级);
- 应采用密码技术保证网络边界访问控制信息的完整性(适用于第四级)。

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设备或组件、密码产品等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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。

网络和通信安全 - 安全接入认证

5.通用测评要求

6.技术测评要求

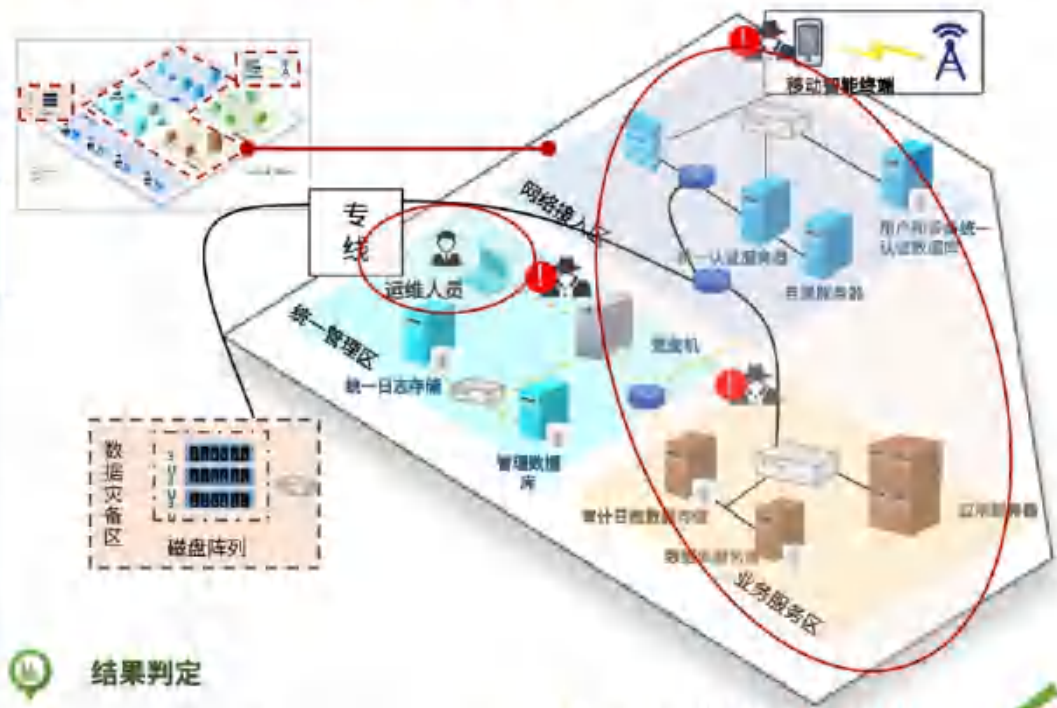
7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则**符合**
- 如果❌为否，则**不符合**
- 其他情况，则为**部分符合**
- 汇总判定结果均为**符合**，则**符合**
- 汇总判定结果均为**不符合**，则**不符合**



测评指标

可采用密码技术对从外部连接到内部网络设备进行接入认证，确保接入设备身份真实性(适用于第三级)；
宜采用密码技术对从外部连接到内部网络设备进行接入认证，确保接入设备身份真实性(适用于第四级)。



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、密码产品等。



测评实施



核查是否符合**密码算法** (5.1)、**密码技术** (5.2) 的要求。



核查是否符合**密码产品** (5.3)、**密码服务** (5.4)、**密钥管理** (5.5) 的要求。



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**有效**。

设备和计算安全 - 身份鉴别



测评指标

可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(适用于第一级)；
宜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(适用于第二级)；
应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(适用于第三级到第四级)。



测评对象

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



测评实施

★ 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。

★ 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。

★ 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，并验证登录设备用户身份真实性实现机制是否正确和有效。



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则符合
- 如果★为否，则不符合
- 其他情况，则为部分符合
- 汇总判定结果均为符合，则符合
- 汇总判定结果均为不符合，则不符合



5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录

设备和计算安全 - 远程管理通道安全

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则**符合**
- 如果否，则**不符合**
- 其他情况，则为**部分符合**
- 汇总判定结果均为**符合**，则**符合**
- 汇总判定结果均为**不符合**，则**不符合**



测评指标

远程管理设备时，应采用密码技术建立安全的信息传输通道(适用于第三级到第四级)。



测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、各类虚拟设备、以及提供安全的信息传输通道的密码产品等。



测评实施

- ★ 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- ★ 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- ★ 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。

设备和计算安全 - 系统资源访问控制信息完整性



测评指标

可采用密码技术保证系统资源访问控制信息的完整性(适用于第一级到第二级);
宜采用密码技术保证系统资源访问控制信息的完整性(适用于第三级);
应采用密码技术保证系统资源访问控制信息的完整性(适用于第四级)。



测评对象

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



测评实施

1 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。

2 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。

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。

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象,其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象,对本单元涉及所有测评对象的判定结果

- 测评内容均为是,则符合
- 如果否,则不符合
- 其他情况,则为部分符合
- 汇总判定结果均为符合,则符合
- 汇总判定结果均为不符合,则不符合

设备和计算安全 - 重要信息资源安全标记完整性

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则符合
- 如果否，则不符合
- 其他情况，则为部分符合
- 汇总判定结果均为符合，则符合
- 汇总判定结果均为不符合，则不符合

测评指标

- 宜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(适用于第三级);
- 应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(适用于第四级)。

测评对象

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

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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。

设备和计算安全 - 日志记录完整性



测评指标

- 可采用密码技术**保证日志记录的完整性**(适用于第一级到第二级);
- 宜采用密码技术**保证日志记录的完整性**(适用于第三级);
- 应采用密码技术**保证日志记录的完整性**(适用于第四级)。



测评对象

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



测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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**确和有效**。

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元如涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为**是**，则**符合**
- 如果**否**，则**不符合**
- 其他情况，则为**部分符合**
- 汇总判定结果均为**符合**，则**符合**
- 汇总判定结果均为**不符合**，则**不符合**

设备和计算安全 - 重要可执行程序完整性、重要可执行程序来源真实性

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果。

- 测评内容均为是，则符合
- 如果否，则不符合
- 其他情况，则为部分符合
- 汇总判定结果均为符合，则符合
- 汇总判定结果均为不符合，则不符合

测评指标

- 宜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(适用于第三级)；
- 应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(适用于第四级)。

测评对象

通用设备、网络及安全设备、密码设备、数据库及其管理系统、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等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 核查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有效。

应用和数据安全 - 身份鉴别



测评指标

- 可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(适用于第一级);
- 宜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(适用于第二级);
- 应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(适用于第三级到第四级)。

测评对象

业务应用, 以及提供身份鉴别功能的密码产品等。

测评实施

- ★ 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- ★ 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- ★ 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登录用户进行身份鉴别,并验证应用系统用户身份真实实现机制是否正确和有效。

结果判定

单个测评对象

- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则**符合**
- 如果★为否, 则**不符合**
- 其他情况, 则为**部分符合**
- 汇总判定结果均为**符合**, 则**符合**
- 汇总判定结果均为**不符合**, 则**不符合**

应用和数据安全 - 访问控制信息完整性

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



测评指标

可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(适用于第一级到第二级);
宜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(适用于第三级);
应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(适用于第四级)。



测评对象

业务应用, 以及提供完整性保护功能密码产品等。



测评实施



核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。



核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。



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。



结果判定

单个测评对象

- 本单元如涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则**符合**
- 如果★为否, 则**不符合**
- 其他情况, 则为**部分符合**
- 汇总判定结果均为**符合**, 则**符合**
- 汇总判定结果均为**不符合**, 则**不符合**

应用和数据安全 - 重要信息资源安全标记完整性

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



测评指标

应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(适用于第三级);
应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(适用于第四级)。

测评对象

业务应用, 以及提供完整性保护功能的密码产品等。

测评实施

★ 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。

★ 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。

★ 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。

结果判定

单个测评对象

- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则符合
- 如果★为否, 则不符合
- 其他情况, 则为部分符合
- 汇总判定结果均为符合, 则符合
- 汇总判定结果均为不符合, 则不符合

应用和数据安全 - 重要数据传输机密性



测评指标

- 可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(适用于第一级);
- 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机密性(适用于第二级);
- 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(适用于第三级到第四级)。

测评对象

业务应用, 以及提供机密性保护功能的密码产品等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 核查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。

结果判定

单个测评对象

- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则**符合**
- 如果 为否, 则**不符合**
- 其他情况, 则为**部分符合**
- 汇总判定结果均为**符合**, 则**符合**
- 汇总判定结果均为**不符合**, 则**不符合**

应用和数据安全 - 重要数据存储机密性



测评指标

- 可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(适用于第一级);
- 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机密性(适用于第二级);
- 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(适用于第三级到第四级)。

测评对象

业务应用, 以及提供机密性保护功能的密码产品等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 核查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。

结果判定

单个测评对象

- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则**符合**
- 如果 为否, 则**不符合**
- 其他情况, 则为**部分符合**
- 汇总判定结果均为**符合**, 则**符合**
- 汇总判定结果均为**不符合**, 则**不符合**

应用和数据安全 - 重要数据传输完整性



测评指标

- 可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(适用于第一级);
- 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(适用于第二级到第三级);
- 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完整性(适用于第四级)。

测评对象

业务应用, 以及提供机密性保护功能的密码产品等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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正确和有效。

结果判定

单个测评对象

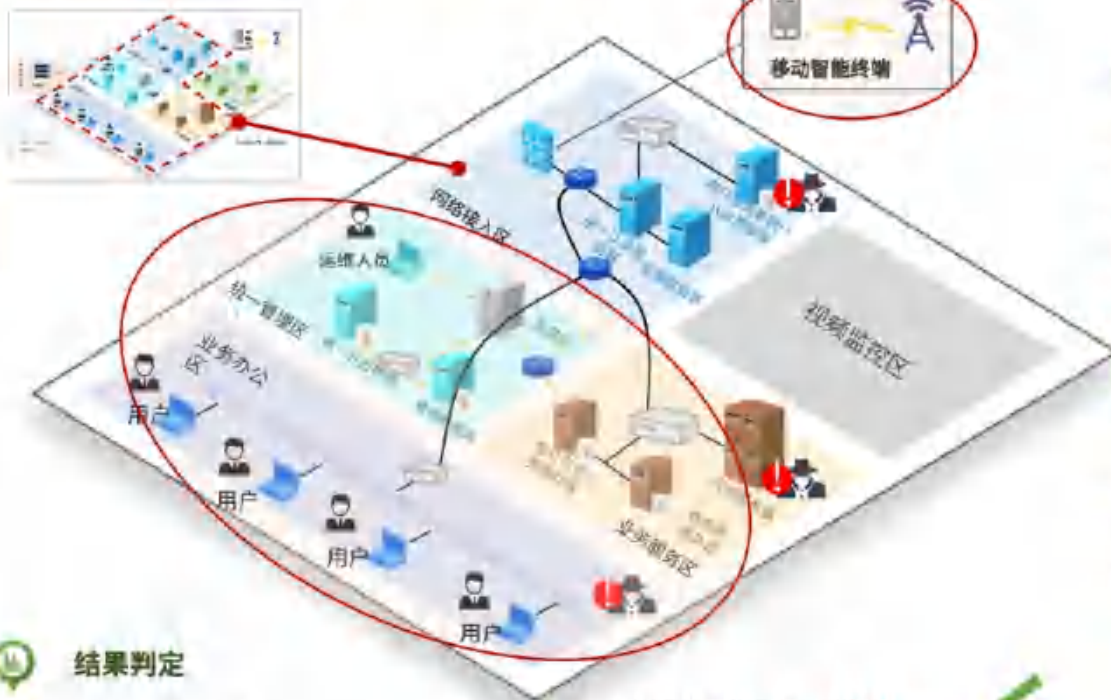
- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则符合
- 如果否, 则不符合
- 其他情况, 则为部分符合
- 汇总判定结果均为符合, 则符合
- 汇总判定结果均为不符合, 则不符合

应用和数据安全 - 重要数据存储完整性



测评指标

- 可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(适用于第一级);
- 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(适用于第二级到第三级);
- 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完整性(适用于第四级)。

测评对象

业务应用, 以及提供机密性保护功能的密码产品等。

测评实施

- 核查是否符合密码算法 (5.1)、密码技术 (5.2) 的要求。
- 核查是否符合密码产品 (5.3)、密码服务 (5.4)、密钥管理 (5.5) 的要求。
- 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正确和有效。

结果判定

单个测评对象

- 本单元只涉及单个测评对象, 其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象, 对本单元涉及所有测评对象的判定结果

- 测评内容均为是, 则**符合**
- 如果★为否, 则**不符合**
- 其他情况, 则为**部分符合**
- 汇总判定结果均为**符合**, 则**符合**
- 汇总判定结果均为**不符合**, 则**不符合**

应用和数据安全 - 不可否认性

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录



结果判定

单个测评对象

- 本单元只涉及单个测评对象，其测评结果即为本单元的测评结果。

本测评单元

- 本单元如涉及多个测评对象，对本单元涉及所有测评对象的判定结果

- 测评内容均为是，则**符合**
- 如果❌为否，则**不符合**
- 其他情况，则为**部分符合**
- 汇总判定结果均为**符合**，则**符合**
- 汇总判定结果均为**不符合**，则**不符合**

测评指标

在可能涉及法律责任认定的应用中，**宜**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(适用于第三级)；

在可能涉及法律责任认定的应用中，**应**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(适用于第四级)。

测评对象

业务应用，以及提供不可否认性功能的密码产品等。

测评实施

★ 核查是否符合**密码算法** (5.1)、**密码技术** (5.2) 的要求。

★ 核查是否符合**密码产品** (5.3)、**密码服务** (5.4)、**密钥管理** (5.5) 的要求。

★ 核查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。

制度管理 - 密码应用安全管理制度、密钥管理规则、操作规程、安全管理制度、管理制度发布流程、制度执行过程记录

5.通用测评要求

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录

制度管理	测评指标	测评对象	测评实施	结果判定
密码应用安全管理制度	应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(适用于第一级到第四级)。	密码应用安全管理制度类文档。	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。	如果测评实施内容均为是,则本单元的测评结果为符合;如果测评实施内容均为否,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。
密钥管理规则	应根据密码应用方案建立相应密钥管理规则(适用于第一级到第四级)。	密码应用方案、密钥管理制度及策略类文档。	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(例如,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。	
操作规程	应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(适用于第二级到第四级)。	操作规程类文档。	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。	
安全管理制度	应定期对密码应用安全管理制度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(适用于第三级到第四级)。	密码应用安全管理制度类文档、操作规程类文档、记录表单类文档。	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。	
管理制度发布流程	应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(适用于第三级到第四级)。	密码应用安全管理制度类文档、操作规程类文档、记录表单类文档。	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。	
制度执行过程记录	应具有密码应用操作规程的相关执行记录并妥善保存(适用于第三级到第四级)。	密码应用安全管理制度类文档、记录表单类文档。	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。	

人员管理 - 密码相关法律法规和密码管理制度、密码应用岗位责任制度

	人员管理	测评指标	测评对象	测评实施	结果判定
5.通用测评要求	密码相关法律法规和密码管理制度	相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度(适用于第一级到第四级)。	信息系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。	核查信息系统相关人员是否熟悉并遵守密码相关法律法规和密码应用安全管理制度	
6.技术测评要求					
7.管理测评要求		a) 应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(适用于第二级)。 b) 应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(适用于第三级): 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应与密钥管理员、密码操作员兼任; 4)相关设备与系统的管理和使用账号不应多人共用。 c) 应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(适用于第四级): 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应与密钥管理员、密码操作员兼任; 4)相关设备与系统的管理和使用账号不应多人共用; 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,并应在任职前对其进行背景调查。	信息应用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、密码安全审计员、密码操作员等)。	a)对于第二级的信息系统,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。 b)对于第三级的信息系统,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、密码安全审计员、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,并确认密码安全审计员岗位人员是否不兼任密钥管理员、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;离职人员及时删除其账号。 c)对于第四级的信息系统,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、密码安全审计员、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,并确认密码安全审计员岗位人员是否不兼任密钥管理员、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;离职人员及时删除其账号;核查密钥管理员、密码安全审计员和密码操作员是否由本机构的内部员工担任,是否具有人员录用时对录用人员身份、背景、专项审查的相关文档或记录等。	如果测评实施内容均为是,则本单元的测评结果为符合;如果测评实施内容均为否,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。
8.整体测评要求					
9.风险分析和评价	密码应用岗位责任制度				
10.测评结论					
附录					

人员管理 - 上岗人员培训制度、安全岗位考核、关键岗位人员保密制度

5.通用测评要求	人员管理	测评指标	测评对象	测评实施	结果判定
6.技术测评要求	上岗人员培训制度	应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(适用于第二级到第四级)。	密码应用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、密码安全审计员、密码操作员等)。	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。	
7.管理测评要求					
8.整体测评要求	安全岗位考核	应定期对密码应用安全岗位人员进行考核(适用于第三级到第四级)。	密码应用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、密码安全审计员、密码操作员等)。	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。	如果测评实施内容均为是,则本单元的测评结果为符合;如果测评实施内容均为否,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。
9.风险分析和评价					
10.测评结论	关键岗位人员保密制度	本单元测评指标如下: ——应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(适用于第一级); ——应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(适用于第二级到第四级)。	密码应用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、密码安全审计员、密码操作员等)。	本单元测评实施如下: a) 对于第一级的信息系统,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; b) 对于第二级到第四级的信息系统,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、责任人的签字等内容。	
附录					

建设运行 - 密码应用方案、密钥安全管理策略、实施方案、投入运行前的密码应用安全性评估、投入运行后的密码应用安全性评估

	建设运行	测评指标	测评对象	测评实施	结果判定
5.通用测评要求	密码应用方案	应根据信息系统密码应用需求和依据密码相关标准,制定密码应用方案(适用于第一级到第四级)。	密码应用方案。	核查在信息系统规划阶段,是否依据信息系统密码应用需求和密码相关标准,制定密码应用方案;并核查方案是否通过评估。	
6.技术测评要求	密钥安全管理策略	应根据密码应用方案,确定系统涉及的密钥种类、体系及其生存周期环节,各环节密钥管理检查要点参照附录A(适用于第一级到第四级)。	密码应用方案、密管理制度及策略类文档、密钥管理过程记录。	a)核查是否有通过评估的密码应用方案;核查密钥管理制度及策略类文档是否确定系统设计的密钥种类、体系及其生存周期环节,是否与密码应用方案一致;如信息系统没有相应的密码应用方案,参照附录A核查密钥管理制度及策略类文档。 b)核查相关密钥管理过程记录,核查是否按照密钥管理制度及策略类文档完成密钥管理。	
7.管理测评要求	实施方案	应按照应用方案实施建设(适用于第一级到第四级)。	密码实施方案。	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。	
8.整体测评要求	投入运行前的密码应用安全性评估	本单元测评指标如下: ——投入运行前可进行密码应用安全性评估(适用于第一级); ——投入运行前宜进行密码应用安全性评估(适用于第二级); ——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(适用于第三级到第四级)。	密码应用安全性评估报告。	本单元测评实施如下: a)对于第一级到第二级的信息系统,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。 b)对于第三级到第四级的信息系统,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。	如果测评实施内容均为是,则本单元的测评结果为符合;如果测评实施内容均为否,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。
9.风险分析和评价	投入运行后的密码应用安全性评估	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(适用于第一级到第四级)。	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	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,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	
10.测评结论					
附录					

应急处置 - 应急策略、事件处置、处置情况上报

	应急处置	测评指标	测评对象	测评实施	结果判定
5.通用测评要求	应急策略	本单元测评指标如下: ——可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(适用于第一级); ——应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(适用于第二级); ——应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,应立即启动应急处置措施,结合实际情况及时处置(适用于第三级到第四级)。	密码应用应急策略、应急处置记录类文档。	本单元测评实施如下。 a)对于第一级的信息系统,检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。 b)对于第二级的信息系统,检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;如发生过密码应用安全事件,检查是否具有相应的处置记录。 c)对于第三级到第四级的信息系统,检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;如发生过密码应用安全事件,检查是否立即启动应急处置措施并具有相应的处置记录。	如果测评实施内容均为是,则本单元的测评结果为符合;如果测评实施内容均为否,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.技术测评要求					
7.管理测评要求					
8.整体测评要求	事件处置	本单元测评指标如下: ——事件发生后,应及时向信息系统主管部门进行报告(适用于第三级); ——事件发生后,应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(适用于第四级)。	密码应用应急策略类文档、安全事件报告。	本单元测评实施如下: a)对于第三级的信息系统,检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; b)对于第四级的信息系统,检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。	
9.风险分析和评价					
10.测评结论					
附录	处置情况上报	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(适用于第二级到第四级)。	密码应用应急策略类文档、安全事件发生情况及处置情况。	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	

整体测评从单元间、层面间等方面进行测评和综合安全分析



整体测评分类

整体测评

单元间测评

指对同一技术层面或管理方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

指对不同技术层面或管理方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。

单元间测评

单元测评完成

应对单元测评结果中存在的不符合项或部分符合项进行单元间测评

重点分析

信息系统中是否
存在同一层面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

不符合项和部分符合项未
导致信息系统整体安全防护能力的缺失

对该测评单元的测评结果予以调整

层面间测评

单元测评完成

应对单元测评结果中存在的不符合项或部分符合项进行层面间测评

重点分析

信息系统中是否
存在不同层面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密码安全防护能力是否缺失

不符合项和部分符合项未
导致信息系统整体安全防护能力的缺失

对该测评单元的测评结果予以调整

密评报告应对整体测评后单元测评结果中不符和部分符合项进行风险分析和评价

风险分析和评价

风险分析

对单元测评结果中存在的不符合项和部分符合项

- 采用风险分析方法分析密码应用在合规性、正确性和有效性方面对应的安全问题被威胁利用的可能性和对信息系统造成的影响
- 综合评价这些不符合项和部分符合项对信息系统带来的不同程度的安全风险

高风险的判定依据

- 不符合项和部分符合项是否会给信息系统带来高安全风险
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合规性、正确性、有效性且存在明显安全风险的情形,例如使用的密码技术不符合法律、法规的规定和密码相关国家标准、行业标准的有关要求,应结合具体业务场景做出高安全风险判定。



测评结论基于整体测评结果和风险分析结果综合给出

5.通用测评要求

信息系统密码应用测评的最终输出是密码应用安全性评估报告，在报告中应描述以下环节的测评情况：各个测评单元的测评结果、整体测评结果、风险分析和评价结果，以及测评结论等。

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录

符合

信息系统所有单元测评结果不存在不符合项和部分符合项。

基本符合

信息系统单元测评结果中存在不符合项和部分符合项，与测评指标存在一定差距，但存在的不符合项和部分符合项未导致信息系统高安全风险。

不符合

信息系统单元测评结果中存在不符合项和部分符合项，与测评指标存在较大差距，或存在的不符合项和部分符合项导致信息系统高安全风险。

附录A：密钥生存周期管理检查要点

5.通用测评要求

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。在信息系统密码应用方案中，需明确信息系统的密钥生存周期管理。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。

6.技术测评要求

7.管理测评要求

8.整体测评要求

9.风险分析和评价

10.测评结论

附录

密钥生存周期	检查目的	检查对象	检查要点
密钥产生	密钥是否在经商用密码认证机构认证的密码产品中产生,密钥协商算法是否经国家密码管理部门核准。	密钥、密钥管理制度及策略类文档,以及密钥存储涉及的密码产品、密码服务以及密码算法实现和密码技术实现。	1) 确认密钥产生所使用的随机数发生器是否具有商用密码认证机构颁发的认证证书; 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。
密钥分发	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。		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何种密码技术保证密钥的机密性、完整性与真实性,并核实采用密码技术的合规性、正确性和有效性。
密钥存储	密钥(除公开密钥)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。		1) 确认系统内部所有密钥(除公开密钥)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(除公开密钥)存储过程中信息系统使用了何种密码技术保证密钥的机密性(除公开密钥)、完整性,并核实采用密码技术的合规性、正确性和有效性; 3) 确认公开密钥存储过程中信息系统使用了何种密码技术保证公开密钥的完整性,正确性和有效性。

附录A：密钥生存周期管理检查要点

	密钥生存周期	检查目的	检查对象	检查要点
5.通用测评要求	密钥使用	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。	密钥、密钥管理制度及策略类文档，以及密钥存储涉及的密码产品、密码服务以及密码算法实现和密码技术实现。	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；
6.技术测评要求				2) 确认信息系统是否具有鉴别公开密钥的真实性与完整性的认证机制，采用的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；
7.管理测评要求				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，是否采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露时，信息系统是否具备应急处理和响应措施；
8.整体测评要求	密钥更新	密钥是否根据相应的更新策略进行更新。		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。
9.风险分析和评价				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。
10.测评结论	密钥归档	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。		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被加密的历史信息或验证被签名的历史信息； 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。

附录A：密钥生存周期管理检查要点

	密钥生存周期	检查目的	检查对象	检查要点
5.通用测评要求				
6.技术测评要求	密钥撤销	公钥证书、对称密钥是否具备撤销机制。	密钥、密钥管理制度及策略类文档，以及密钥存储涉及的密码产品、密码服务以及密码算法实现和密码技术实现。	1) 如信息系统内部使用公钥证书、对称密钥,则确认是否有公钥证书、对称密钥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。
7.管理测评要求	密钥备份	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。		1) 如信息系统内部存在需要备份的密钥，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，信息系统使用了何种密码技术保证备份密钥的机密性、完整性； 3) 确认是否包括备份主体、备份时间等密钥备份的审计信息。
8.整体测评要求	密钥恢复	密钥是否具备恢复机制，并生成审计信息。		1) 确认信息系统内部是否具有密钥的恢复机制并有效执行； 2) 确认是否包括恢复主体、恢复时间等密钥恢复的审计信息。
9.风险分析和评价				
10.测评结论	密钥销毁	密钥是否具备销毁机制，销毁过程是否具备不可逆性。		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：典型密码功能测评技术

5.通用测评要求	密码功能	对应测评单元	可能涉及的密码产品	测评实施要点	预期结果
6.技术测评要求	传输机密性	6.2.3、6.3.2、6.4.4	IPSec/SSL VPN(互联网安全协议/安全套接层虚拟专用网)网关、密码机、智能密码钥匙等	1) 利用协议分析类工具，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)是否与信息系统实际使用的密码技术相符合； 2)如果信息系统以外挂密码产品的形式实现传输机密性，如VPN网关、密码机、智能密码钥匙，见附录C中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)与信息系统实际使用的密码技术相符合； 2)实现传输机密性的密码产品在信息系统中被动正确使用且提供的传输机密性功能有效
7.管理测评要求					
8.整体测评要求					
9.风险分析和评价	存储机密性	6.4.5	密码机、智能密码钥匙等	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(如分组长度等)是否与信息系统实际使用的密码技术相符合； 2)如果信息系统以外挂密码产品的形式实现存储机密性，如密码机、智能密码钥匙，见附录C中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(如分组长度等)与信息系统实际使用的密码技术相符合； 2)实现存储机密性的外挂密码产品在信息系统中被正确使用且提供的存储机密性功能有效
10.测评结论					

附录B：典型密码功能测评技术

密码功能	对应测评单元	可能涉及的密码产品	测评实施要点	预期结果
5.通用测评要求	传输完整性	IPSec/SSLVPN网关、密码机、智能密码钥匙等	1) 利用协议分析类工具，分析被完整性保护的数据在传输时的数据格式(如签名长度、消息鉴别码的长度)是否与信息系统实际使用的密码技术相符合； 2) 如果采用数字签名技术进行完整性保护，可使用公钥对抓取的签名结果进行验证； 3) 如果信息系统以外挂密码产品的形式实现传输完整性，如VPN网关、密码机、智能密码钥匙，见附录C中对这些密码产品应用的测评方法	1) 被完整性保护的数据在传输时的数据格式(如签名长度、消息鉴别码的长度)与信息系统实际使用的密码技术相符合； 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挂密码产品在信息系统中被正确使用且提供的传输完整性功能有效
6.技术测评要求				
7.管理测评要求				
8.整体测评要求	存储完整性	电子门禁系统、视频监控系統、密码机、智能密码钥匙等	1) 通过读取存储的重要数据，判断被完整性保护的数据在存储时的数据格式(如签名长度、消息鉴别码的长度)是否与信息系统实际使用的密码技术相符合； 2) 如果采用数字签名技术进行完整性保护，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，可尝试对存储数据进行篡改(如修改消息鉴别码或数字签名结果)，验证完整性保护措施的有效性； 4) 如果信息系统以外挂密码产品的形式实现存储完整性保护，如电子门禁系统、视频监控系統、密码机、智能密码钥匙，见附录C中对这些密码产品应用的测评方法	1) 被完整性保护的数据在存储时的数据格式(如签名长度、消息鉴别码的长度)与信息系统实际使用的密码技术相符合； 2) 使用签名技术进行完整性保护时，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挂密码产品在信息系统中被正确使用且提供的存储完整性功能有效
9.风险分析和评价				
10.测评结论				

附录B：典型密码功能测评技术

密码功能	对应测评单元	可能涉及的密码产品	测评实施要点	预期结果
5.通用测评要求	真实性	6.1.1、 6.2.1、6.2.5、 6.3.1、6.3.2、 6.3.6、6.4.1	电子门禁系统、IPSec/SSL VPN网关、安全认证网关、动态令牌系统等	1) 实现对用户、设备的真实性鉴别的外挂密码产品在信息系统中被正确使用且提供的真实性功能有效。
6.技术测评要求				2) 实体鉴别机制符合GB/T15843(所有部分)中的要求。
7.管理测评要求				3) 对于口令鉴别方式，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。如果采用了数字证书，应符合证书认证系统相关要求。
8.整体测评要求				4) 公钥和(对称)密钥与实体的绑定方式可靠，部署过程安全
9.风险分析和评价	不可否认性	6.4.8	智能密码钥匙、证书认证系统、电子签章系统等	1) 使用的第三方电子认证密码服务符合相关要求；
10.测评结论				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) 实现不可否认性的密码产品在信息系统中被正确使用且提供的不可否认性功能有效

更新解读

01 密评背景介绍

02 密评总体要求

03 密评测评要求

04 密评方案要求

05 密评测评过程

06 密评团标解读

07 密改FAQ解读

08 密改方案实践



标准提出了信息系统密码应用设计相关参考建议



标准内容

本文件给出了信息系统密码应用设计指南，包括信息系统密码应用框架、密码应用方案设计原则、密码应用方案设计过程和密码应用方案设计指南

适用范围

本文件适用于指导信息系统密码应用方案的设计，也可作为信息系统密码保障建设、密码应用安全性评估和密码管理部门密码应用安全性评估备案工作的参考

引用文件

GB/T 22240《信息安全技术 网络安全等级保护定级指南》、GB/T 25069《信息安全技术 术语》、GB/T 39786《信息安全技术 信息系统密码应用基本要求》

术语定义

密码应用方案，是指用于指导信息系统责任主体合规、正确、有效地使用密码技术，部署密码保障系统的规划

使用密码保护的信息系统密码应用框架图

1.密码应用框架

2.方案设计原则

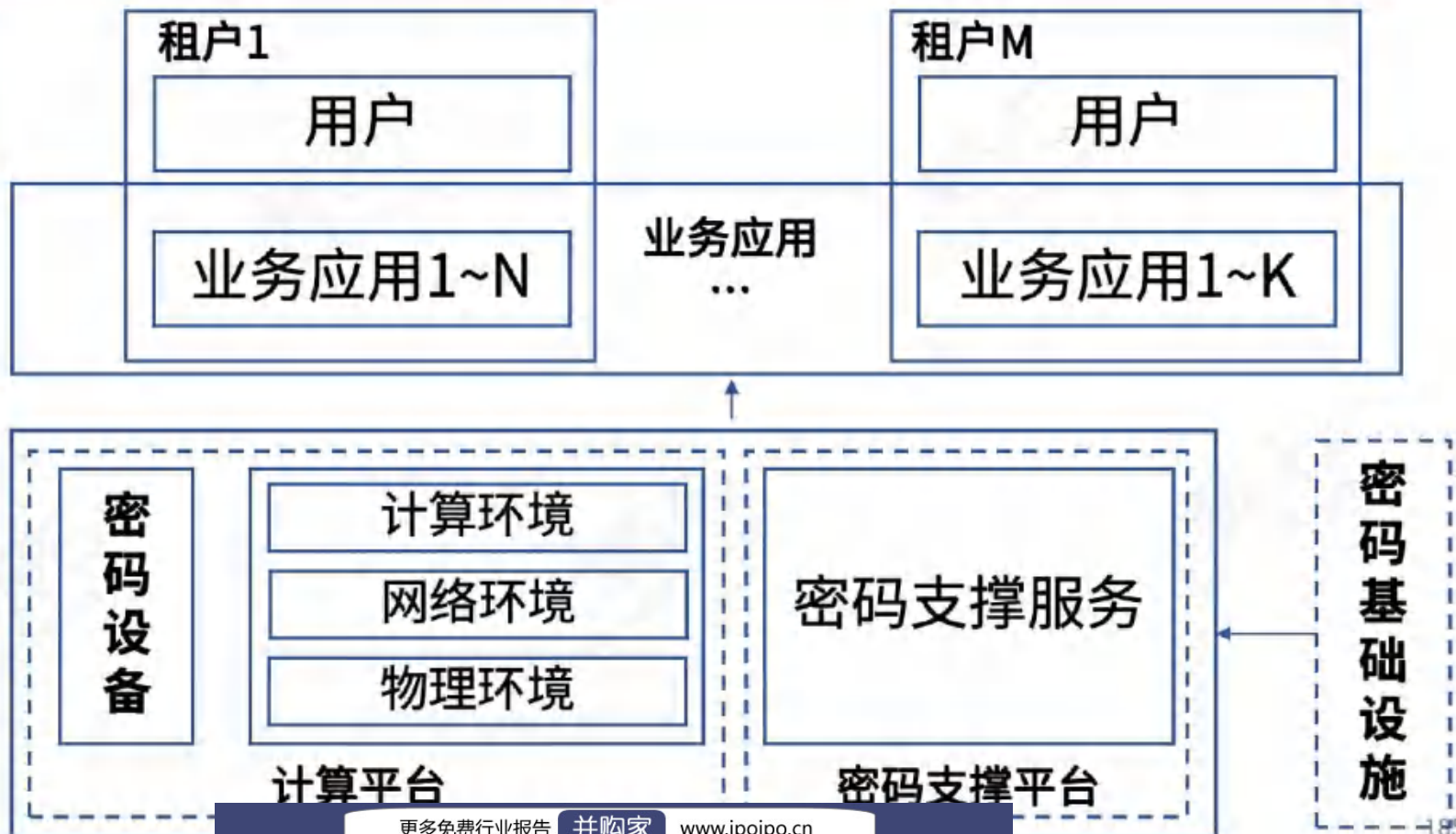
3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南



信息系统包括计算平台的运营方、密码支撑平台的服务提供方和租户等主体

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

信息系统密码应用框架中涉及的计算平台、密码支撑平台、业务应用、用户和租户如下:

框架组成	主要介绍
计算平台	是承载业务应用的物理环境、网络环境和计算环境。物理环境提供机房、供电、通风、空调、门禁和监控等保障条件;网络环境为业务应用提供数据传输通道和通信设备;计算环境提供承载业务应用运行和数据存储的设备或服务。计算平台中部署的密码设备(也可使用密码支撑平台提供的密码功能),为计算平台的运行安全和管理安全提供密码保障。
密码支撑平台	为计算平台上运行的各类业务应用提供密码支撑服务,该服务以接口的形式提供密码功能,供各业务应用调用,以解决各业务应用的安全问题。密码基础设施为密码应用提供基础支撑。
业务应用	是运行在计算平台上,实现业务功能的计算机程序。业务应用的密码应用安全对应GB/T 39786中的应用和数据安全。业务应用为解决安全问题需要使用的密码功能,由密码支撑平台提供。计算平台上可运行有多个业务应用,各个业务应用的安全需求各不相同,所以每个业务应用都需要有各自的密码应用设计。
用户	是业务应用的使用者,用户端使用的计算机设备安全,属于计算平台安全,用户计算机上运行的业务系统客户端安全,属于应用安全。
租户	是业务应用的所有者和用户的管理者。可有多租户,每个租户可管理多个业务应用,各个业务应用可有不同的用户群。租户还承担着所属业务应用及其相应的密码管理职责。

信息系统密码应用方案设计需遵循总体性、科学性、完备性等五大原则

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

信息系统密码应用方案设计原则如下:

五大设计原则	详情介绍
总体性原则	按照 GB/T 39786 对信息系统密码应用的基本要求, 以及信息系统的安全需求责任单位的密码应用规划和密码管理需求, 进行顶层设计
科学性原则	参考信息系统的 密码需求、管理需求和整体规划 , 合理整合和部署密码资源, 切实解决应用中的安全问题
完备性原则	依据法律、法规、标准等关于密码使用的要求, 设计 满足信息系统安全需求 的密码应用方案
可行性原则	密码应用方案 切合实际、便于实现 , 能作为信息系统密码应用建设、验收和密码应用安全性评估的依据
合规性原则	密码应用方案中使用的密码算法遵循国家有关法律法规的要求; 使用的密码技术遵循国家及行业相关标准; 涉及国家安全、国计民生、社会公共利益的信息系统, 其使用的密码产品和服务经商用密码认证机构认证合格

密码应用设计首先需确定信息系统的安全需求

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

密码应用需求分析

密码应用设计分析

安全与合规性分析

需求背景分析

分析信息系统现状，明确需要保护的信息资源和所涉及的范围，确定信息系统的安全需求

明确技术和管理要求

依据GB/T 22240中等级保护定级，按照GB/T 39786中对不同等级的信息系统提出的密码应用基本要求，针对信息系统建设的安全策略和业务安全需求，明确密码应用技术要求和管理要求

不采用密码技术情况

对使用其他替代性风险控制措施而不采用密码技术的，做出相应的说明并在密码应用方案设计时进行风险评估和论证

密码应用设计分析主要参考GB/T 22240、GB/T 39786等标准要求

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

密码应用需求分析

密码应用设计分析

安全与合规性分析

等级保护

参照

标准：《GB/T 22240 信息安全技术 网络安全等级保护定级指南》

注：参照该标准中等级保护定级

应用设计

根据

被保护对象的密码需求

在GB/T 39786中所处的层面

对应等级下GB/T 39786对该对象的密码应用基本要求

进行密码设计

计算平台密码应用方案设计

密码支撑平台方案设计

业务应用的密码应用方案设计

并从信息系统的以下四个方面提出密码应用管理要求

应用管理

管理制度

人员管理

建设运行

应急处置

注：方案设计过程中可能用到的标准参见附录B

安全与合规性分析需对照GB/T 39786具体技术要求，对方案适用性进行检查

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

密码应用需求分析

密码应用设计分析

安全与合规性分析

逐条对照

标准：《GB/T 39786 信息安全技术 信息系统密码应用基本要求》对应等级下的各项密码应用技术要求

进行检查

对方案的适用性进行检查

逐条对照

GB/T 39786 对应等级下的各项密码应用技术要求

满足条件则该指标的自评结果为通过

指标涉及的所有保护对象的相应安全控制措施(密码保障措施、缓解及替代性措施)有效、不存在高风险

且

方案中描述的
实施保障
措施合理

判断为
“适用”

以下场景可能
“不适用”

有下列情况时，对应的指标可为“不适用”，对于不适用的项，做出相应的说明：

- 1) GB/T 39786 中有“应”“宜”的指标项而实际信息系统中不存在对应对象，指标项可为“不适用”；
- 2) GB/T 39786 中有“宜”的指标项，信息系统采用替代性风险控制措施满足风险控制需求，指标项可为“不适用”；
- 3) GB/T 39786 中有“可”的指标项，信息系统责任方自行决定是否采用密码技术保护指标涉及的保护对象，若决定不采用密码技术保护指标涉及的保护对象，指标项可为“不适用”。

计算平台的物理环境密码应用安全对应 GB/T 39786 中的物理和环境安全

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

计算平台密码应用方案

密码支撑平台方案

业务应用密码方案

物理和环境安全

参考标准 对应 **GB/T 39786 中的物理和环境安全**

保护对象 ① 物理访问身份鉴别 ② 电子门禁记录数据 ③ 视频监控记录数据

应用设计 按照 GB/T 39786 基本要求 实际环境的具体需求 机房等重要区域 电子门禁记录数据 视频监控记录数据 进行密码应用设计

设计内容 选择的密码技术和标准 采用的密码设备 密码设备的部署位置 and 方式 密码设备的使用和管理

网络和通信安全

参考标准 对应 **GB/T 39786 中的网络和通信安全**

保护对象 信息系统与外界交互的**通信信道**

应用设计 按照 GB/T 39786 基本要求 实际环境的具体需求 需要密码保护的每一条通信信道 进行密码应用设计

设计内容 选择的密码技术和标准 采用的密码设备 密码设备的部署位置 and 方式 密码设备的使用和管理

注：需要接入认证的设备，根据具体情况选择使用的密码技术，确定在设备端和认证设备端的密码应用需求和部署

设备和计算安全

参考标准 对应 **GB/T 39786 中的设备和计算安全**

保护对象 信息系统中承载业务应用的**计算环境**，包括**信息技术产品**

应用设计 按照 GB/T 39786 基本要求 实际环境的具体需求 需要保护的**对象** 进行密码应用设计

设计内容 选择的密码技术和标准 采用的密码设备 密码设备的部署位置 and 方式 密码设备的使用和管理

计算平台的网络环境密码应用安全对应 GB/T 39786 中的网络和通信安全

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

计算平台密码应用方案

密码支撑平台方案

业务应用密码方案

平台作用

为承载在计算平台上的各类业务应用提供密码功能服务

选择
产品

可选择采用经认证合格的密码支撑服务产品（如密码服务平台等）

也可根据各类应用的密码需求、性能需求 and 责任主体的规划要求等，基于经认证合格的密码产品进行设计

设计的内容如下表所示

序号	关键词	具体设计内容
1	服务机构	密码服务机构的确定、接入方式和服务策略
2	体制算法	支持的密码体制和密码算法
3	遵循标准	接口和功能遵循的标准
4	功能提供	提供的密码支撑方式（如租密码机方式、租密码服务器方式和租密码服务方式）；提供的密码功能及接口（如实体鉴别、签名验签和加密解密），也可提供密码应用服务（如时间戳、电子印章和安全认证网关）
5	功能部署	部署的位置和方式（如部署的位置、部署的方式、使用和管理等内容），部署的方式包括全网统一部署和分租户分散部署
6	接入方式	接入计算平台的方式（如独立的形态，不占用计算平台的任何资源；非独立的形态，借用或租用计算平台的计算资源和网络资源）
7	密钥管理	密钥管理方式，按责任主体的规划要求确定（如租户自行管理，支撑平台提供管理界面；租户委托管理，支撑平台代管密钥）
8	平台安全	租户间的隔离安全等

计算平台的计算环境密码应用安全对应 GB/T 39786 中的设备和计算安全

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A
应用方案模板

附录B
标准使用指南

附录C
策略设计指南

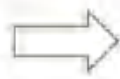
计算平台密码应用方案

密码支撑平台方案

业务应用密码方案

保护对象

信息系统中的所有应用及其重要数据



应用设计

按照

GB/T 39786基
本要求
各业务系统实
际需求

需要保护的
对象

进行密
码应用
设计

设计的内容如下表所示

序号	关键词	具体设计内容
1	确定密码体制	按照信息系统的规划、责任主体的需求、现有或规划的密码功能提供模式，确定密码体制
2	梳理业务流程	梳理业务流程，根据流程安全需求，为关键环节设计密码保护机制
3	梳理业务数据	梳理业务数据，根据数据安全需求，为重要数据设计密码保护机制
4	梳理业务对象	梳理业务对象（如文件、证照、票据、病历、采集的数据和控制指令等），根据安全需求，为其设计密码保护机制
5	设计保护机制	根据角色和访问控制，为其权限和访问策略等设计密码保护机制；根据审计策略，为日志记录设计密码保护机制
6	设计管理策略	为角色分配密钥，明确密钥载体，设计系统的密钥管理策略；
7	功能属性指明	使用加密功能的，需指明密码算法、加密模式、数据填充方式和密钥属性等；使用签名功能的，需指明签名算法和签名机制（如签名内容、签名主体和签名位置等）；使用完整性保护功能的，需指明使用的算法和校验机制
8	数据结构修改	根据保护机制，修改被保护对象的数据结构，将上述内容添加到原数据结构中，使其成为带安k全机制的数据结构
9	功能设计支撑	实现保护机制用到的密码功能和用户登录用到的身份鉴别功能，由密码支撑平台提供，数据传输和数据存储安全，的，可设计信源加密机制

附录A：密码应用方案模板

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A 应用方案模板

附录B 标准使用指南

附录C 策略设计指南

一级标题	二级标题	具体内容
1.密码应用框架	背景	明确系统的建设规划、国家有关法律法规要求、与规划有关的前期情况概述和项目实施的必要性，以及信息系统相关的其他情况说明。
	基本情况	系统基本情况包括系统名称、系统责任主体单位情况、系统上线运行时间、系统用户情况、是否为关键信息基础设施、等级保护定级和备案情况、网络安全等级测评情况以及密码应用安全性评估情况等。
	系统概述	如果密码应用方案包括计算平台密码应用方案设计，则包括物理环境、网络环境、计算环境等具体描述；如果密码应用方案不包括计算平台密码应用方案设计，则描述计算平台的场所地点和密码应用安全性评估情况
	业务应用现状 密码应用现状 应用管理现状	主要包括业务应用的基本情况、承载的业务情况，且对于多个子应用的信息系统，对每个子应用分别描述 信息系统部署密码设施设备的基本情况、责任主体和密码支撑情况等 管理要求包括信息系统管理制度、人员管理、建设运行和应急处置等
2.方案设计原则	应用需求分析	结合信息系统现状和 GB/T 39786 中对不同等级的信息系统提出的密码应用基本要求，对密码应用方案涉及的计算平台、业务应用、管理制度、人员管理、建设运行和应急处置进行安全风险分析，确定风险控制措施、密码应用基本需求分析和密码应用特殊需求分析。通过风险控制措施缓解信息系统存在的高风险
	安全目标及设计原则	提出密码应用方案所涉及对象的密码应用安全目标
	设计原则与依据	提出密码应用方案的设计原则，遵循的政策法规和相关标准
	密码应用技术框架	包括密码应用技术框架图及框架说明。密码应用技术框架包括计算平台、密码支撑平台和业务应用密码应用架构等，综合描述各平台、系统之间的关系，清晰展示密码应用整体技术框架
3.方案设计过程	计算平台密码应用方案	密码应用方案涉及计算平台安全
	密码支撑平台方案	密码应用方案涉及为业务应用提供密码功能
	业务应用的密码应用方案	密码应用方案涉及业务应用安全
	密码应用部署	包括软硬件设备清单（软硬件设备均需包括已有的密码产品清单）、部署示意图及说明等。新增加的密码设备需要明确标识
4.方案设计指南	安全管理方案	参照 GB/T 22240 中等级保护定级，根据 GB/T 39786 对该等级的管理要求根据部署的密码产品管理机制，设计安全管理方案，包括管理制度、人员管理、建设运行和应急处置方面的制度
	安全与合规性分析	逐条对照 GB/T 39786 对应等级下的各项密码应用基本要求，对方案的适用情况采取的密码保障措施、采取的缓解及替代性措施及自评结果进行说明
	实施内容	描述实施对象的边界及密码应用的范围、任务要求等。实施内容包括但不限于采购、软硬件开发或改造、系统集成、综合调试和试运行等。分析项目实施的重难点问题，提出实施过程中可能存在的风险点及应对措施
	实施计划	包括实施路线图、进度计划和重要节点等。按照施工进度计划确定实施步骤，并分阶段描述任务分工、实施主体、项目建设单位和阶段交付物等
附录A 应用方案模板	实施保障方案	包括项目实施过程中的组织保障、人员保障、经费保障、质量保障和监督检查等措施
	保障措施	

附录B.1: 密码支撑类标准

	接口及功能类型	密码应用场景	可遵循的标准
1.密码应用框架	接口调用	密码支撑平台通过接口提供密码功能，业务应用通过接口调用密码功能	GB/T 38629 信息安全技术 签名验签服务器技术规范
2.方案设计原则			GM/T 0019 通用密码服务接口规范
3.方案设计过程			GM/T 0020 证书应用综合服务接口规范
			GM/T 0033 时间戳接口规范
4.方案设计指南	实体鉴别协议	应用系统调用密码功能，按照标准实现身份鉴别协议	GM/T 0067 基于数字证书的身份鉴别接口规范
			GB/T 15843(所有部分) 信息技术 安全技术 实体鉴别
			GB/T 38556 信息安全技术 动态口令密码应用技术规范
			GM/T 0067 基于数字证书的身份鉴别接口规范
附录A 应用方案模板	加解密、签名、验签和完整性计算	应用系统调用密码功能，按照标准对数据加密、解密、签名验签、计算消息鉴别码	GM/T 0069 开放的身份鉴别框架
			GM/T 0113 在线快捷身份鉴别协议
			GB/T 15852(所有部分) 信息技术 安全技术 消息鉴别码
附录B 标准使用指南	基础标准	应用系统调用密码功能时，指明算法和用法	GB/T 17964 信息安全技术 分组密码算法的工作模式
		应用系统管理用户实体时，关联用户的数字证书	GB/T 35276 信息安全技术 SM2密码算法使用规范
附录C 策略设计指南			应用系统对数据加密或签名
			GB/T 20518 信息安全技术 公钥基础设施 数字证书格式
			GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规则

附录B.2-B.3：密码应用类及测评类标准

	密码应用场景	可遵循的标准
1.密码应用框架	业务应用	GB/T 38541 信息安全技术 电子文件密码应用指南
2.方案设计原则		GB/T 39786 信息安全技术 信息系统密码应用基本要求
		GM/T 0055 电子文件密码应用技术规范
		GM/T 0099 开放式版式文档密码应用技术规范
		GM/T 0111 区块链密码应用技术要求
3.方案设计过程	GM/T 0112 PDF格式文档的密码应用技术要求	
	构建授权与访问控制机制	GM/T 0032 基于角色的授权与访问控制技术规范
4.方案设计指南	使用/验证电子印章、电子签章	GB/T 38540 信息安全技术 安全电子签章密码技术规范
		GB/T 32922 信息安全技术 IPsec VPN 安全接入基本要求与实施指南
	部署密码产品或密码系统	GB/T 38540 信息安全技术 安全电子签章密码技术规范
		GM/T 0023 IPsec VPN 网关产品规范
		GM/T 0025 SSL VPN 网关产品规范
附录A 应用方案模板		GM/T 0026 安全认证网关产品规范
附录B 标准使用指南	信息系统密码应用安全性评估 相关标准（含指导文件）	GM/T 0036 采用非接触卡的门禁系统密码应用技术指南
		GM/T 0096 射频识别防伪系统密码应用指南
GM/T 0115 信息系统密码应用测评要求		
附录C 策略设计指南		GM/T 0116 信息系统密码应用测评过程指南

附录C：密钥管理策略设计指南

1.密码应用框架

2.方案设计原则

3.方案设计过程

4.方案设计指南

附录A 应用方案模板

附录B 标准使用指南

附录C 策略设计指南

序号	策略设计步骤	对应步骤设计内容参考
1	密钥产生	密钥在符合 GB/T 37092 规定的密码产品中产生。明确信息系统中密钥的产生方式和来源，密钥产生的同时记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间和使用终止时间等。
2	密钥分发	密钥分发时保证密钥的机密性、完整性以及分发者、接收者身份的真实性等，确定密钥与实体的关联关系，并建立密钥介质的管理规范。
3	密钥存储	明确各类型密钥存储的位置和方式，如密钥在符合 GB/T 37092 的密码产品中存储，或者在对密钥进行机密性和完整性保护后，存储在通用设备或系统中。除公钥外，密钥不以明文方式存储在密码产品外部并采取严格的安全防护措施，防止密钥被非授权的访问或篡改。公钥可以明文方式存储在密码产品外部，但有必要采取安全防护措施，防止公钥被篡改。
4	密钥使用	明确各类型密钥的使用要求并按要求使用密钥，包括使用条件、时间和用途等。密钥一般在符合 GB/T 37092 规定的密码产品内部产生，且每个密钥一般只有单一的用途。公钥使用前需要验证其完整性，以及与实体的关联关系，确保公钥来源的真实性。
5	密钥更新	设定密钥更新策略，包括密钥的更新周期、更新机制、更新流程，以及保障密钥更新前后业务连续性的措施，并指定密钥更新人员。在密钥超过使用期限、泄露或存在泄露风险时，根据相应的密钥更新策略进行更新。
6	密钥归档	如果信息系统有密钥归档需求，明确密钥归档的条件、人员和流程，并确定归档密钥的存储位置、存储方式以及管理者。根据安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。归档密钥只能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。执行密钥归档时，生成审计信息，包括归档的密钥和归档的时间等。
7	密钥撤销	明确密钥的撤销条件、撤销流程、撤销机制和撤销人等，以及撤销后密的处理方式等。
8	密钥备份	指定备份操作人员、备份密钥管理人员、备份密钥管理机制、备份密钥恢复流程以及备份密钥存档要求等。明确密钥备份的机密性、完整性以及与实体和其他信息的关联关系。对密钥备份过程进行记录，并生成审计信息，审计信息包括备份的主体和备份的时间等。
9	密钥恢复	制定密钥恢复要求与机制，确定密钥恢复流程，指定密钥恢复操作员。对密钥恢复过程进行记录，并生成审计信息，审计信息包括恢复的主体和恢复的时间等。
10	密钥销毁	制定密钥销毁相关要求，根据密钥存储介质情况确定密钥销毁模式，明确密钥销毁机制、销毁启动条件（设备失控、丢弃时进

01 密评背景介绍

02 密评总体要求

03 密评测评要求

04 密评方案要求

05 密评测评过程

06 密评团标解读

07 密改FAQ解读

08 密改方案实践



《GM/T 0116-2021信息系统密码应用测评过程指南》

GB/T 25069—2010
信息安全技术 术语

GM/T 0115 信息系统密码
应用测评要求

GM/Z 4001 密码术语

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

规范性引用文件

信息系统密码应用测评过程指南

范围

本标准规定了信息系统密码应用的测评过程，规范了测评活动及其工作任务

本标准适用于商用密码应用安全性评估机构、信息系统责任单位开展密码应用安全性评估工作

术语定义

GB/T 25069—2010和GM/Z 4001中界定的以及下列术语和定义适用于本文件。

测评方：对信息系统开展密码应用安全性评估（简称“密评”）的主体，具体可以是商用密码应用安全性评估机构或信息系统责任单位

被测单位：信息系统责任单位

商用密码应用安全性评估人员（简称“密评人员”）：指测评方中从事测评活动的人员

测评方对信息系统开展密评的基本原则



客观公正性原则

测评实施过程中，测评方应保证在符合国家密码管理部门要求及最小主观判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测评活动。



可重用性原则

测评工作可重用已有测评结果，包括商用密码检测认证结果和密码应用安全性评估的测评结果等。所有重用结果都应以已有测评结果仍适用于当前被测信息系统为前提，并能够客观反映系统当前的安全状态。



可重复性和可再现性原则

依照同样的要求，使用同样的测评方法，在同样的环境下，不同的密评人员对每个测评实施过程的重复执行应得到同样的结果。可重复性和可再现性的区别在于，前者关注同一密评人员测评结果的一致性，后者则关注不同密评人员测评结果的一致性。



结果完善性原则

在正确理解GM/T 0115各个要求项内容的基础之上，测评所产生的结果应客观反映信息系统的密码应用现状。测评过程和结果应基于正确的测评方法，以确保其满足要求。

测评开始前及测评过程面临的风险



验证测试可能影响被测信息系统正常运行

在现场测评时，需对设备和系统进行一定的验证测试工作，部分测试内容需上机查看信息，可能对被测信息系统的运行造成不可预期的影响。



工具测试可能影响被测信息系统正常运行

在现场测评时，根据实际需要可能会使用一些测评工具进行测试。测评工具使用时可能会产生冗余数据写入，同时可能会对系统的负载造成一定的影响，进而对被测信息系统中的服务器和网络通信造成一定影响甚至损害。



可能导致被测信息系统敏感信息泄漏

测评过程中，可能泄露被测信息系统的敏感信息，如加密机制、业务流程、安全机制和有关文档信息等。



其他可能面临的风险

在测评过程中，也可能出现影响被测信息系统可用性、机密性和完整性的风险。

测评过程中规避风险应采取的措施

三个签署

签署委托测评协议书

在测评工作正式开始之前，测评方和被测单位需要以委托协议的方式，明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务。

签署保密协议

测评相关方应签署合乎法律规范的保密协议，规定测评相关方在保密方面的权利、责任与义务。

签署现场测评授权书

现场测评之前，测评方应与被测单位签署现场测评授权书，要求测评相关方对系统及数据进行备份，采取适当的方法进行风险规避，并针对可能出现的事件制定应急处理方案。

一个要求

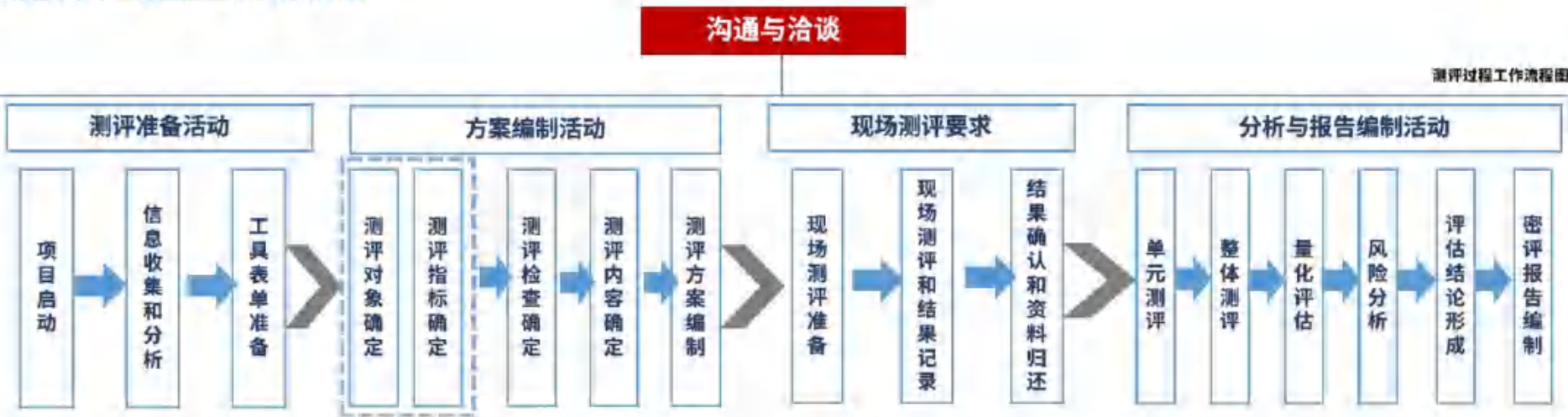
现场测评要求

验证测试和工具测试时，避开被测信息系统业务高峰期，在系统资源处于空闲状态时进行测试，或配置与被测信息系统一致的模拟/仿真环境，在模拟/仿真环境下开展测评工作；需进行上机验证测试时，密评人员应提出需要验证的内容，由被测单位的技术人员进行实际操作。整个现场测评过程，由被测单位和测评方相关人员进行全程监督。

测评工作完成后，密评人员应交回在测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档，并将测评现场环境恢复至测评前状态。

测评过程整体流程

测评过程工作流程图



测评准备活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制密评方案做好准备。

方案编制活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等，形成密评方案，为实施现场测评提供依据。

现场测评要求是开展测评工作的核心活动，主要任务是根据密评方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够的证据，发现其存在的密码应用安全性问题。

分析与报告编制活动是给出测评工作结果的活动的，主要任务是根据密评方案和GM/T 0115的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成密评报告。

测评准备活动总体输出文档

任务	输出文档	文档内容
项目启动	项目计划书	项目概述、工作依据、技术思路、工作内容和项目组织等
信息收集和分析	完成的调查表格，各种与被测信息系统相关的技术资料	被测信息系统的网络安全保护等级、业务情况、软硬件情况、密码应用情况、密码管理情况和相关部门及角色等
工具和表单准备	选用的测评工具清单，打印的各类表单，如现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等	测评工具、现场测评授权、测评可能带来的风险、交接的文档名称、会议记录、会议签到信息等

项目启动



项目启动

信息收集和分析

工具表单准备

输入

委托测评协议书、保密协议

任务
描述

a) 根据测评委托测评协议书和被测信息系统规模，测评方组建测评项目组，编制项目计划书。项目计划书应包含项目概述、工作依据、技术思路、工作内容和项目组织等内容

b) 测评方要求被测单位提供基本资料，为全面初步了解被测信息系统做好资料准备（具体要求见扩展附录1——附录4）

输出

项目计划书

扩展附录一：被测系统情况《商用密码应安全性评估报告模板（2023版）》

1. 承载的业务情况	2. 网络拓扑图及描述	3. 密码应用情况			
		物理和环境安全密码应用情况	网络和通信安全密码应用情况	设备和计算安全密码应用情况	应用和数据安全密码应用情况
主要介绍信息系统承载的业务情况，重点说明业务的密码应用需求	主要介绍信息系统的完整网络拓扑，方便了解信息系统边界、资产等基本情况	介绍物理和环境安全层面密码应用的大致情况。考虑到该层面的密码应用流程和密钥管理主要由 密码产品完成 ，且与信息系统承载的业务关联性较低，因此可以主要围绕所使用的密码产品展开介绍	介绍网络和通信安全层面密码应用的大致情况。考虑到该层面的密码应用流程和密钥管理主要由 VPN等密码产品完成 ，因此可以主要围绕所使用的密码产品展开介绍	介绍设备和计算安全层面密码应用的大致情况。考虑到该层面的密码应用流程和密钥管理主要由密码产品完成，且与信息系统承载的业务关联性较低，因此可以主要围绕所使用的密码产品展开介绍	详细介绍应用和数据安全层面的密码应用情况。 这部分是重点，与信息系统承载的业务息息相关，建议分为密码应用工作流程和密钥体系两方面分别介绍

扩展附录二：被测系统资产模版《商用密码应安全性评估报告模板2023版》

表6 数据库管理系统

序号	数据库管理系统名称	版本	部署位置	主要功能	重要程度
1					
2					
3					
4					
5					

表7 关键业务应用

序号	应用名称	版本	部署位置	主要功能
1				
2				
3				
4				
5				

表8 密码服务

序号	密码服务名称	密码服务提供商
1		
2		

表9 重要数据

序号	数据	描述	所属应用	存储位置	安全需求
1					机密性/真实性/完整性
2					
3					

表10 安全管理文档

序号	文档名称	主要内容
1		
2		
3		

表11 人员

序号	姓名	岗位/角色	职责说明	联系方式
1				
2				
3				

具体要求：信息收集和分析

项目启动

信息收集和分析

工具表单准备

输入

调查表格

任务描述

a) 测评方收集测评所需资料：

测信息系统总体描述文件、被测信息系统密码应用总体描述文件、网络安全等级保护定级报告、安全需求分析报告、安全总体方案、安全详细设计方案、密码应用方案、相关密码产品的用户操作指南、各种密码应用安全规章制度，以及相关过程管理记录和配置管理文档等。

b) 测评方将被测信息系统基本情况调查表格提交给被测单位，协助并督促被测信息系统相关人员准确填写调查表格。

c) 测评方收回填写完成的调查表格，并分析调查结果，了解和熟悉被测信息系统的实际情况。分析的内容包括被测信息系统的基本信息、行业特征、~~密码应用部署~~、网络及设备部署、软硬件重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、被测信息系统~~密码安全保护等级~~、用户类型、用户类型、~~被测信息系统~~等。以上信息可以采信自查结果、上次网络安全保护等级测评报告或商用密码应用安全性评估报告中的可信结果。

d) 如果调查表格中有填写不准确、不完善或存在相互矛盾的情况，密评人员应与填表人进行沟通和确认。~~必要时，测评方应安排现场调查，收集与被测信息系统相关人员就进行现场确认~~，以确保调查信息的正确性和完整性。

输出

具体要求：工具和表单准备

项目启动

信息收集和分析



工具表单准备

输入

完成的调查表格，各种与被测信息系统相关的技术资料

任务描述

a) 校准本次测评过程中将用到的测评工具

b) 如果具备条件，建议密评人员模拟被测信息系统搭建测评环境，进行前期准备和验证，为方案编制活动、现场测评活动提供必要的条件

c) 准备并打印表单，主要包括：现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等

输出

调查表格

方案编制活动总体输出文档

任务	输出文档	文档内容
测评对象确定	密评方案的测评对象部分	被测信息系统的整体结构、边界、网络区域、核心资产、面临的威胁、测评对象等
测评指标确定	密评方案的测评指标部分	被测信息系统相应等级对应的适用和不适用的测评指标
测评检查点确定	密评方案的测评检查点部分	测评检查点、检查内容及测评方法
测评内容确定	密评方案的单元测评实施部分	单元测评实施内容
密评方案编制	经过评审和确认的密评方案文本	项目概述、测评对象、测评指标、测评检查点、单元测评实施内容、测评实施计划等

主要任务：测评对象确定

测评对象确定

测评指标确定

测评内容确定

测评检查点确定

密评方案编制

输入

完成的调查表格，各种与被测信息系统相关的技术资料

5个任务描述

a) 识别被测信息系统的基本情况

根据调查表格获得的被测信息系统情况，识别出被测信息系统的物理环境、网络拓扑结构和外部边界连接情况、业务应用系统，以及与其相关的重要的计算机硬件设备、网络安全设备、密码产品和使用的密码服务等，并识别与上述内容相关的密码应用情况。

b) 描述被测信息系统

对识别出的被测信息系统的基本情况进行整理，并对被测信息系统进行描述。描述被测信息系统时，一般以被测信息系统的网络拓扑结构为基础，采用总分式的描述方法，先说明整体结构，然后描述外部边界连接情况和边界主要设备，最后介绍被测信息系统的网络区域组成、主要业务功能及相关的设备节点，同时务必描述在这些方面所识别的密码应用情况。

c) 确定测评对象

根据被测信息系统的重要程度及其相关设备和组件等情况，明确核心资产在被测信息系统内的流转，从而确定与密码相关的测评对象。
被测单位需要确定被测信息系统需要保护的核心资产，以及相应的威胁模型和安全策略。核心资产可以是业务应用、业务数据或者业务应用的某些设备、组件。核心资产及其他需要保护的配套数据（如审计信息、配置信息、访问控制列表等）、敏感安全参数（主要指密钥）的威胁模型和安全策略等均由被测单位根据密码应用方案、网络安全等级保护定级报告等确定，并由测评方进行核查和确认。

主要任务：测评对象确定

测评对象确定

测评指标确定

测评内容确定

测评检查点确定

密评方案编制

↓ 接上页任务描述

d)资产和威胁评估

资产价值根据资产重要性和关键程度确定。资产价值分为高、中、低三个等级。

资产价值高低的界定，可由被测单位根据密码应用方案、网络安全等级保护定级报告等继承和确定，并由测评方进行核查和确认。

对于各类资产和其他敏感信息，测评方与被测单位需要分析其可能面临的威胁及威胁发生的频率。威胁发生的频率分为高、中、低三个等级。

可能面临的威胁以及威胁发生的频率，可由被测单位根据密码应用方案、网络安全等级保护定级报告等继承和确定，并由测评方进行核查和确认。

d) 描述测评对象

测评对象包括机房、业务应用软件、主机和服务、数据库、网络安全设备、密码产品、密码服务、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）及安全管理制度类文档和记录表单类文档等。在对每类测评对象进行描述时一般采用列表的方式，如对硬件设备进行描述时，应包括测评对象所属区域、设备名称、用途、设备信息等内容。

输出

主要任务：测评指标确定

测评对象确定



测评指标确定

测评内容确定

测评检查点确定

密评方案编制

↓ 输入

完成的调查表格，GM/T 0115，通过评估的密码应用方案，相关行业标准或规范

任务描述

a)根据被测信息系统的调查表格，获得被测信息系统的定级结果，并根据GM/T 0115选择相应等级对应的测评指标。

b)根据被测信息系统相关的行业标准或规范，以及被测信息系统密码应用需求，确定特殊测评指标。

c)对于核心资产、物理环境及其他需要保护的数据（如密钥、鉴别数据等），应按照被测信息系统的安全策略、相关标准要求进行逐项确认。通过确认在核心资产、物理环境及其他需要保护的数据全生命周期流转过程中**所涉及的密码算法、密码技术、密码产品、密码服务等，明确密钥生存周期管理相关的要求**，并对照已通过评估的密码应用方案逐项确认各项指标的适用性。

d)如果确无密码应用方案，则需要对所有不适用项进行逐条核查、评估，详细论证其安全需求、不适用的具体原因，以及是否采用了可满足安全要求的其他替代性风险控制措施来达到等效控制（具体模版见扩展附录5）。

输出

扩展附录三：不适用指标《商用密码应安全性评估报告模板2023版》

*鉴于信息系统的复杂性和特殊性，GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第{X}级要求中的个别项可能不适用于被测信息系统，对于这些不适用项及其不适用原因如下表所示：

表 3-2 不适用指标及说明

安全层面	测评指标	测评指标描述	不适用原因
物理和环境			
网络和通信			
设备和计算			
.....			
不适用项合计			

主要任务：测评内容确定

测评对象确定

测评指标确定



测评内容确定

测评检查点确定

密评方案编制



输入

完成的调查表格，密评方案的测评对象、测评指标及测评检查点部分，通过评估的密码应用方案和GM/T 0115

任务描述

依据通过评估的密码应用方案和GM/T 0115，首先将已经得到的测评指标与测评对象结合起来。

其次将测评对象与具体的测评方法结合起来，具体做法：

- 1) 将各层面上的测评指标结合到具体的测评对象上，并说明具体的测评方法，构成若干个可以具体实施测评的单元。
- 2) 然后，结合已选定的测评指标和测评对象，概要说明现场单元测评实施的工作内容；涉及现场测试部分时，应根据确定的测评检查点，编制相应的测试内容。
- 3) 在密评方案中，现场单元测评实施内容通常以表格的形式给出，表格内容包括测评指标、测评内容描述等。

输出

主要任务：测评检查点确定

测评对象确定

测评指标确定

测评内容确定

测评检查点确定

密评方案编制



输入

被测信息系统详细网络结构，选用的密码算法、密码技术、密码产品、密码服务等详细信息，通过评估的密码应用方案和GM/T 0115

任务描述

a) 关键设备检查是现场测评的重要环节，关键设备一般为承载核心资产流转、进行密钥管理的设备。密评人员应列出需要接受现场检查的关键设备和检查内容，包括：涉及密码的部分是否使用国家密码管理部门认可的密码算法、密码技术、密码产品和密码服务等；相关配置是否与密码应用需求相符；是否满足GM/T 0115中的相关条款要求等。

b) 在使用工具进行测评时（测评工具包括但不限于：协议分析工具、算法合规性检测工具、随机性检测工具和数字证书格式合规性检测工具等），应在保证被测信息系统正常、安全运行的情况下，确定测试路径和工具接入点，并结合网络拓扑图，采用图示的方式描述测评工具的接入点、测试目的、测试途径和测试对象等相关内容。当从被测信息系统边界外接入时，测试工具一般接在系统边界设备（通常为交换机）上；从系统内部不同网段接入时，测试工具一般接在与被测对象不在同一网段的内部核心交换机上；从系统内部同一网段接入时，测试工具一般接在与被测对象在同一网段的交换机上。当测评工具接入被测信息系统条件不成熟时，测评方应与被测单位协商、配合，生成必要的离线数据。

输出

主要任务：密评方案编制

测评对象确定

测评指标确定

测评内容确定

测评检查点确定

密评方案编制

↓ 输入

委托测评协议书、项目计划书、完成的调查表格、通过评估的密码应用方案和GM/T 0115，密评方案中测评对象、测评指标、测评检查点、测评内容等部分

任务描述

a)根据委托测评协议书和完成的调查表格，提取项目来源、被测单位整体信息化建设情况及被测信息系统与其他系统之间的连接情况等。

b)结合被测信息系统的实际情况，根据通过评估的密码应用方案和GM/T 0115，明确测评活动所要依据和参考的与密码算法、密码技术、密码产品和密码服务等相关的标准规范。

c)依据委托测评协议书和被测信息系统的情况，估算现场测评工作量，具体可根据配置检查的节点数量、工具测试的接入点及测试内容等情况进行估算。

d)根据测评项目组成员分工，编制工作安排。

e)根据以往测评经验以及被测信息系统规模，编制具体测评实施计划，包括现场工作人员的分工和时间安排。在进行时间安排时，应尽量避免被测信息系统的业务高峰期，避免给被测信息系统的正常运行带来影响。同时，在测评计划中应将具体测评工作所需的人员、资料、场所等保障要求一并提出，以确保现场测评工作的顺利开展。

f)汇总上述内容及方案编制活动中其他任务获取的内容，形成密评方案。

g)密评方案经测评方内部评审通过后，提交被测单位签字确认。

输出

现场测评活动总体输出文档

任务	输出文档	文档内容
现场测评准备	会议记录、更新确认的密评方案、签署过的测评授权书和风险告知书等	工作计划和内容安排、双方人员的协调、被测单位应提供的配合与支持等
现场测评和结果记录	各类测评结果记录	访谈、文档审查、实地察看和配置检查、工具测试的记录及测评结果
测评结果确认和资料归还	经过被测单位确认的各类测评结果记录	测评活动中发现的问题、问题的证据和证据源、每项测评活动中被测单位配合人员的书面认可文件

主要任务：现场测评准备

现场测评准备

现场测评和结果记录

结果确认和资料归还

↓ 输入

现场测评授权书，经过评审和确认的密评方案，风险告知书等

任务描述

a)召开测评现场首次会，测评方介绍测评工作，进一步明确测评计划和方案中的内容，说明测评过程中具体实施的工作内容、测评时间安排、测评过程中可能存在的安全风险等。

b)测评方与被测单位确认现场测评所需的各种资源，包括被测单位的配合人员和需要提供的测评条件等，确认被测信息系统已备份过系统及相关数据。

c)被测单位签署现场测评授权书和风险告知书。

d)密评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

↓ 输出

主要任务：现场测评和结果记录

现场测评准备

现场测评和结果记录

结果确认和资料归还

↓ 输入

更新确认后的密评方案，测评结果记录表格，各种与被测信息系统相关的技术资料

任务描述

a) 测评方安排密评人员在约定的测评时间，通过与被测信息系统有关人员（个人/群体）的访谈、文档审查、实地察看，以及在测评检查点进行配置检查和工具测试等方式，测评被测信息系统是否达到了相应等级的要求。

b) 对于已经取得相应证书的密码产品，测评时不对其本身进行重复检测，主要进行符合性核验和配置检查，对于存在符合性疑问的，可联系密码产品审批部门或相应的检测认证机构加以核实。

c) 进行配置检查时，根据被测单位出具的商用密码产品认证证书（复印件）、安全策略文档或用户手册等，首先确认实际部署的密码产品与声称情况的一致性，然后查看配置的正确性，并记录相关证据。如果存在不明确的问题，可由被测单位通知密码产品厂商现场提供证据（如密码产品送检文档等）

d) 见下一页

↓ 输出

主要任务：现场测评和结果记录

现场测评准备

现场测评和结果记录

结果确认和资料归还

接上页任务描述

d) 进行工具测试时，需根据被测信息系统的实际情况选择测试工具，在配置检查无法提供有力证据的情况下，应通过工具测试的方法抓取并分析被测信息系统相关数据。以下列出了数据采集和分析的几种方式：

1) 需要重点采集被测信息系统与外界通信的数据以及被测信息系统内部传输和存储的数据，分析使用的密码算法、密码协议、关键数据结构（如数字证书格式）是否合规，检查传输的口令、用户身份数据等敏感数据是否进行了保护（如明文传输、明文加密传输、重要关键数据是否以明文出现），验证设备密钥是否按照要求生成；在条件允许的情况下，可以重放采集的关键数据（如身份鉴别数据）验证被测信息系统是否具备防重放攻击的能力，或者修改传输的数据验证被测信息系统是否对传输数据进行了完整性保护。

2) 为了验证密码产品是否被正确、有效地使用，可采集密码产品及其调用者之间的通信数据，通过采集的密码产品调用指令和响应报文，分析密码产品的调用是否符合预期（比如密码计算请求是否实时发起，数据内容和长度是否符合逻辑）；若无法在密码产品和调用者之间接入测试工具（比如密码产品是软件密码模块），且被测信息系统无法提供源代码等有关证据的情况下，可通过逆向分析等方法对被测信息系统应用程序进行逆向分析，探究应用程序内部组成结构及工作原理，核查应用程序调用密码功能的合理性。

3) 在不影响被测信息系统正常运行的情况下，探测IPSec VPN和SSL VPN等密码协议所对应的特定端口服务是否开启，利用漏洞扫描、渗透测试等工具对被测信息系统进行分析，查看被测信息系统是否存在与密码相关的安全漏洞。

输出

主要任务：结果确认和资料归还

现场测评准备

现场测评和结果记录

结果确认和资料归还

↓ 输入

测评结果记录，工具测试完成后的电子输出记录

任务描述

a) 密评人员在现场测评完成之后，应首先汇总现场测评的测评记录，对遗漏和需要进一步验证的内容实施补充测评。

b) 召开测评现场结束会，测评方与被测单位对测评过程中得到各类测评结果记录进行现场沟通和确认。

c) 测评方归还测评过程中借阅的所有文档资料，将测评现场环境恢复至测评前状态，并由被测单位文档资料提供者签字确认。

↓ 输出

分析与报告编制活动总体输出文档

任务	输出文档	文档内容
单元测评	密评报告的单元测评部分	汇总统计各测评指标的各个测评对象的测评结果，给出单元测评结果
整体测评	密评报告的单元测评结果修正部分	分析被测信息系统整体安全状况及对各测评对象测评结果的修正情况
量化评估	密评报告中整体测评结果和量化评估部分，以及总体评价部分	综合单元测评和整体测评结果，计算得分，并对被测信息系统的密码应用情况安全性进行总体评价
风险分析	密评报告的风险分析部分	分析被测信息系统存在的安全问题风险情况
评估结论形成	密评报告的评估结论部分	对测评结果进行分析，形成评估结论
密评报告编制	经过评审和确认的密评报告	测评项目概述、被测系统情况、测评范围与方法、单元测评、整体测评、量化评估、风险分析、评估结论、总体评价、安全问题及改进建议等

分析与报告编制活动主要任务：单元测评

单元测评

整体测评

量化评估

风险分析

评论结论形成

密评报告编制

↓ 输入

经过被测单位确认的各类测评结果记录，GM/T 0115

任务描述

a)按照GM/T 0115，针对各测评单元涉及的各个测评对象，将实际获得的多个测评结果与预期的测评结果相比较，分别判断每个测评结果与预期结果之间的符合性，**综合判定该测评对象的测评结果**，从而得到每个测评对象对应的测评结果，**包括符合、不符合、部分符合和不适用四种情况。**

b)按照GM/T 0115，汇总各测评单元涉及的所有测评对象的测评实施结果，对各测评单元进行结果判定，判别原则如下：

- 1)测评单元包含的所有测评对象的测评结果均为符合，则对应测评单元结果判定为符合。
- 2)测评单元包含的所有测评对象的测评结果均为不符合，则对应测评单元结果判定为不符合。
- 3)测评单元包含的所有测评对象的测评结果均为不适用，则对应测评单元结果判定为不适用。
- 4)测评单元包含的**所有测评对象的测评结果不全为符合或不符合**，则对应测评单元结果**判定为部分符合**。

输出

扩展附录四：单元测评之密码技术应用要求《商密应安全性评估报告模板2023版》

物理和环境安全

结果汇总：

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表所示：

表 物理和环境安全测评结果汇总

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	电子门禁记录数据存储完整性	视频监控记录数据存储完整性
1	{XXXX 机房}			
2	{YYYY 机房}			
单元测评结果 (符合/部分符合/不符合/不适用)				

结果分析：

{主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。}

扩展附录五：单元测评之密码技术应用要求《商用密码应用安全性评估报告模板2023版》

应用和数据安全

结果汇总：针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表1所示：

表 1 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）						不可否認性
		身份鉴别	访问控制	重要信息传输安全标记完整性	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	
1	（应用层业务系统）							
2	其他							
单元测评结果 （符合/部分符合/不符合/不适用）								

针对应用和数据安全层面重要数据的机密性和完整性保护情况进行说明和汇总，如表3所示：

表 3 应用和数据安全重要数据测评结果汇总

序号	重要数据	传输机密性	存储机密性	传输完整性	存储完整性
1	（应用层业务系统）				
2	（应用层业务系统）				
3	（应用层业务系统）				
4	（应用层业务系统）				
5	（应用层业务系统）				
6	（应用层业务系统）				
7	（应用层业务系统）				
8	（应用层业务系统）				
9	（应用层业务系统）				
单元测评结果 （符合/部分符合/不符合/不适用）					

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2所示：

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

针对应用和数据安全层面不可否認性情况进行说明和汇总，如表 4 所示：

表 4 应用和数据安全不可否認性测评结果汇总

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

结果分析：

{主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及

判定依据等。}

227

扩展附录七：单元测评之安全管理《商用密码应用安全性评估报告模板2023版》

建设运行

结果汇总：针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表1所示：

表1 建设运行测评结果汇总

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）				
		制定密码应用方案	制定密钥安全管理策略	制定实施方案	投入运行前进行密码应用安全性评估	定期开展密码应用安全性评估及攻防对抗演习
1	{密码应用方案、密钥管理制定及策略类文档、密码类方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档}					
2	{管理体系（包括安全管理规章制度文档、记录表单类文档、系统相关人员）}					
单元测评结果 (符合/部分符合/不符合/不适用)						

结果分析：

{主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。}

应急处置

结果汇总：针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表2所示：

表2 应急处置测评结果汇总

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）		
		应急策略	事件处置	向有关主管部门上报处置情况
1	{管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员）}			
单元测评结果 (符合/部分符合/不符合/不适用)				

结果分析：

{主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。}

分析与报告编制活动主要任务：整体测评

单元测评

整体测评

量化评估

风险分析

评论结论形成

密评报告编制

↓ 输入

密评报告的单元测评部分

任务描述

a) 针对测评对象“部分符合”及“不符合”要求的单个测评项，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，发生何种关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果（模版见扩展附录11）。

b) 针对测评对象“部分符合”及“不符合”要求的单个测评项，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，发生何种关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

c) 结合单元测评的结果汇总和整体测评结果，将物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等层面中各个测评对象的测评结果再次汇总分析，统计符合情况。

输出

扩展附录八：测评结果修正《商用密码应安全性评估报告模板2023版》

测评结果修正模版

序号	安全层面	测评单元	测评对象	经弥补前的测评结果/分值	经弥补后的测评结果/分值 ^a	弥补原因及相关测评对象
1	应用和数据安全	重要数据传输机密性	对象1	{不符合0}	{部分符合0.5}	{示例：该测评对象在应用和数据安全层面明文传输。测评对象原始分值为0，在网络和通信安全层面，通过部署经商用密码检测认证的SSL/VPN建立安全传输通道（网密SSL协议），对传输数据进行机密性保护，分值为1分，经网络和通信安全层面弥补后，该测评对象分值为0.5。}
			对象2	{部分符合0.25}	{部分符合0.5}	
2		测评单元2	对象1			
						
						

风险分析模版

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	身份鉴别：.....。			1	0	0
2		电子门禁记录数据存储完整性：.....。					
3		视频监控记录数据存储完整性：.....。					
4							
统计							

主要任务：量化评估

单元测评

整体测评

量化评估

风险分析

评论结论形成

密评报告编制

↓ 输入

密评报告的单元测评的结果汇总及整体测评部分

任务描述

a) 根据整体测评结果，计算修正后的各测评指标的各个测评对象的测评结果符合程度得分。

b) 根据各个测评对象的符合程度得分，计算各测评单元得分。

c) 根据各测评单元得分，计算各安全层面得分。

d) 根据各安全层面得分，计算整体得分。

e) 根据各测评单元、各层面和整体得分，总体评价被测信息系统已采取的有效保护措施和存在的密码应用安全问题情况。

输出

扩展附录九：整体测评结果模版《商用密码应用安全性评估报告模板2023版》

层面 (类)	测评单元	符合情况				测评单元 得分 S_{ij}	安全层面得分 情况 $S_i = \frac{\sum_{j=1}^n w_{ij} S_{ij}}{\sum_{j=1}^n w_{ij}}$
		符合	部分符合	不符合	不适用		
物理和环境安全	身份鉴别						
	电子门禁记录数据存储空间完整性						
	视频监控记录数据存储空间完整性						
网络和通信安全	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						
	安全接入认证						
设备和计算安全	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						
应用和数据安全	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						
管理制度	不可否认性						
	具备密码应用安全管理制度						
	密钥管理规则						
	建立操作规程						

人员管理	定期修订安全管理制度						
	明确管理制度发布流程						
	制度执行过程记录留存						
	了解并遵守密码相关法律法规和密码管理制度						
	建立密码应用岗位责任制度						
	建立上岗人员培训制度						
	定期进行安全岗位人员考核						
建设运行	建立关键岗位人员保密制度和调离制度						
	制定密码应用方案						
	制定密钥安全管理策略						
	制定实施方案						
	投入运行前进行密码应用安全性评估						
	定期开展密码应用安全性评估及攻防对抗演习						
应急处置	应急策略						
	事件处置						
	向有关主管部门上报处置情况						
合计							
符合情况		符合	部分符合	不符合	不适用	综合得分 $\frac{\sum_{i=1}^n w_i \cdot S_i}{\sum_{i=1}^n w_i} \times 100$	

主要任务：风险分析

单元测评

整体测评

量化评估

风险分析

评论结论形成

密评报告编制

↓ 输入

完成的调查表格，密评报告的整体测评结果和量化评估部分，相关风险评估标准

任务描述

a) 根据威胁类型和威胁发生频率，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。

b) 根据资产价值的高低，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测信息系统的业务信息安全造成的影响程度，影响程度取值范围为高、中和低。

c) 结合前两步分析结果，测评方根据自身经验和相关标准或文件，对被测信息系统面临的密码应用安全风险进行赋值，风险值的取值范围为高、中和低。

d) 结合被测信息系统的网络安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。如果存在高风险项，则认为被测信息系统面临高风险；同时也需要考虑多个中低风险叠加后可能导致的高风险问题。

输出

主要任务：评论结论形成要求

单元测评

整体测评

量化评估

风险分析

评论结论形成

密评报告编制

↓ 输入

密评报告中被测信息系统的综合得分和总体评价部分，风险分析部分

任务描述

***根据被测信息系统的综合得分和风险分析结果，得出评估结论。评估结论分为以下三种情况**

a)符合：被测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：被测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被测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：被测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，而且存在的安全问题会导致被测信息系统面临高等级安全风险，或者综合得分低于阈值。

输出

主要任务：密评报告编制

单元测评

整体测评

量化评估

风险分析

评论结论形成

密评报告编制

↓ 输入

完成的调查表格，密评方案，单元测评的结果汇总部分，整体测评部分，总体评价部分，风险分析部分，评估结论部分等

任务描述

a) 密评人员整理各项任务输出，编制密评报告相应部分。对每一个定级的被测信息系统应单独形成一份密评报告。

b) 针对**被测信息系统存在的安全问题**，提出相应改进建议，并编制密评报告安全文件及改进建议部分。

c) 采取列表方式给出现场测评文档清单和测评记录，以及对各个测评项的测评结果判定情况，编制密评报告单元测评的结果记录、整体测评结果、风险分析和评估结论等部分内容。

d) 密评报告编制完成后，测评方应根据委托测评协议书、被测单位提交的相关文档、测评原始记录和其他辅助信息，对密评报告进行内部评审。

e) 密评报告通过内部评审后，由授权签字人进行签发，提交被测单位。

输出

《商用密码应用安全性评估报告模板（2023版）》

《商用密码应用安全性评估报告模板（2023版）》更新发布



发布机构：中国密码学会密评联委会

发布时间：2023年1月20日

修订说明：《商用密码应用安全性评估报告模板（2023版）》用于替代2021年12月发布的《商用密码应用安全性评估报告模板（2021版）》，供相关单位参考。

《商用密码应用安全性评估报告模版》2021版对比2023版

2021版vs2023版

九处增加点，四处修改点

报告编号: {}

XXXXX **系统**

商用密码应用安全性评估报告

被测单位: _____

密评机构: _____

报告时间: _____

2021版vs2023版

六处增加点

报告编号: {}

《XXX 系统密码应用**方案**》

商用密码应用安全性评估报告

委托单位: _____

密评机构: _____

报告时间: _____

2023版《密评报告模版》之系统密评报告模版修改点总览

“被测系统基本信息表”增加两处内容

- a) 增加被测系统是否属于关键信息基础设施板块
- b) 增加系统是否依赖不在本系统范围内的云平台运行板块

“总体评价”中增加测评结果模版

1.3.1测评准备阶段，“表1-1测评项目组成员”增加“是否通过密评人员考核”

“表2-1物理环境”增加“XX机房”示例；表2-2物理安防设施增加“电子门禁系统和视频监控系统”等产品名称

“2.7前次密评情况”增加上次密评机构、综合得分

“表6-1风险分析”增加“安全层面”和“问题描述”示例

报告模板增加“附录B密评活动有效性证明记录”

九处增加点

四处修改点

被测系统基本信息表中密码应用方案
密评方式由“专家评审”改为“自行评估”其他“评审”改为“评估”

“表2-12安全威胁”，威胁层面改为安全层面

“附录A”，密码使用安全D改为密码使用有效性D

2021版与2023版系统密评模版“被测信息系统基本信息表”对比

商用密码应用安全性评估报告模板

2021

被测信息系统基本信息表

被测单位			
单位名称		单位名称	
单位地址		邮政编码	
所属主管部门			
联系人	姓名	职务/职称	
	所属部门	办公电话	
	移动电话	电子邮箱	
被测信息系统			
系统名称			
网络安全等级保护定级情况 ☐ 已定级，第__级（一至四级），S_A_G__ ☐ 未定级，本次密评按照GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》第__级（一至四级）信息系统要求			
网络安全等级保护定级备案情况 ☐ 已备案 备案证明编号： ☐ 未备案		本次被测信息系统与密评保护定级系统是否一致 ☐ 是 ☐ 否，变化情况说明：	
网络安全等级保护测评情况 ☐ 已测评 测评机构名称： 测评时间： 测评结论： ☐ 通过测评 ☐ 未测评			
系统服务范围		系统服务情况	
☐ 全国 ☐ 跨省（区、市）跨__个 ☐ 全省（区、市） ☐ 跨地（市、县）跨__个 ☐ 地（市、县）内 ☐ 其他		☐ 金融 ☐ 广电 ☐ 能源信息公共互联网 ☐ 铁路 ☐ 银行 ☐ 海关 ☐ 税务 ☐ 民航 ☐ 电力 ☐ 证券 ☐ 保险 ☐ 国防科技工业 ☐ 公安 ☐ 邮政 ☐ 人力资源和社会保障 ☐ 审计 ☐ 商务贸易 ☐ 国土资源 ☐ 能源 ☐ 交通 ☐ 统计 ☐ 工商行政管理 ☐ 粮食 ☐ 教育 ☐ 文化 ☐ 卫生 ☐ 农业 ☐ 水利 ☐ 气象 ☐ 其他	

新增

合并

定级和备案情况

内容无变化

排版形式改变

被测信息系统基本信息表

被测单位			
单位名称		单位名称	
单位地址		邮政编码	
所属主管部门			
联系人	姓名	职务/职称	
	所属部门	办公电话	
	移动电话	电子邮箱	
被测信息系统			
系统名称			
是否由关键信息基础设施 ☐ 已认定，所属安全保护工作部门： ☐ 未认定			
☐ 已定级备案，第__级（一至四级），S_A_G__ 备案证明编号： 本次被测信息系统与密评保护定级系统是否一致： ☐ 是 ☐ 否，变化情况说明： ☐ 未定级，本次密评按照GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》第__级（一至四级）信息系统要求			
网络安全等级保护定级和备案情况		网络安全等级保护测评情况	
☐ 已测评 测评机构名称： 测评时间： 测评结论：		☐ 未测评	
系统服务范围		系统服务情况	
☐ 全国 ☐ 跨省（区、市）跨__个 ☐ 全省（区、市） ☐ 跨地（市、县）跨__个 ☐ 地（市、县）内 ☐ 其他		☐ 金融 ☐ 广电 ☐ 能源信息公共互联网 ☐ 铁路 ☐ 银行 ☐ 海关 ☐ 税务 ☐ 民航 ☐ 电力 ☐ 证券 ☐ 保险 ☐ 国防科技工业 ☐ 公安 ☐ 邮政 ☐ 人力资源和社会保障 ☐ 审计 ☐ 商务贸易 ☐ 国土资源 ☐ 能源 ☐ 交通 ☐ 统计 ☐ 工商行政管理 ☐ 粮食 ☐ 教育 ☐ 文化 ☐ 卫生 ☐ 农业 ☐ 水利 ☐ 气象 ☐ 其他	

商用密码应用安全性评估报告模板

2023

2021版与2023版系统密评模版“被测信息系统基本信息表”对比

商用密码应安全性评估报告模板

2021

商用密码应安全性评估报告模板

2023

服务对象	☐ 中华人民共和国公民 ☐ 社会公共人员 ☐ 两省均包括其他		
系统网络平台	覆盖范围 ☐ 局域网 ☐ 广域网 ☐ 广域网 ☐ 其他 网络性质 ☐ 业务专用 ☐ 互联网 ☐ 其他		
系统服务用户数量	大概数量级/被控系统处于建设阶段		
系统是否已投入运行	☐ 是，投入运行时间： 年 月 ☐ 否，目前情况：		
系统互联情况	☐ 与基础支付系统连接 ☐ 与金融行业其他系统连接 ☐ 与本单位其他系统连接 ☐ 其他		
系统是否具有密码应用方案	☐ 有密码应用方案，且通过密评，密评机构名称： ☐ 有密码应用方案，但未通过密评 ☐ 无密码应用方案		
系统使用的密码产品情况	☐ 系统使用的密码产品（含/不含），独立使用（含/不含），共享使用（含/不含）； 其中，取得认证证书的密码产品数量（含/不含），未取得认证证书的国产密码产品数量（含/不含），国外产品数量（含/不含）。		
系统使用的密码算法	对称算法： ☐ SM1 ☐ SM4 ☐ SM7 ☐ AES ☐ DES ☐ 3DES ☐ 其他 非对称算法： ☐ SM2 ☐ SM9 ☐ RSA1024 ☐ RSA2048 ☐ 其他 杂凑算法： ☐ SM3 ☐ SHA-1 ☐ SHA-256 ☐ SHA-384 ☐ SHA-512 ☐ MD5 ☐ 其他 序列算法： ☐ ZUC ☐ 其他 其他算法：		
密评机构			
单位名称			
通信地址			邮政编码
联系人	姓名	职务/职称	
	所属部门	办公电话	
	移动电话	电子邮箱	
审核批准	审核人（签字）	审核日期	
	审核人（签字）	审核日期	
	审核人（签字）	审核日期	

新增
互联网系统名称
“专家评审”修改为
“自行评估”
新增
系统未使用密码产品

系统网络平台	覆盖范围 ☐ 局域网 ☐ 广域网 ☐ 广域网 ☐ 其他 网络性质 ☐ 业务专用 ☐ 互联网 ☐ 其他		
系统服务用户数量	大概数量级/被控系统处于建设阶段		
系统是否已投入运行	☐ 是，投入运行时间： 年 月 ☐ 否，目前情况：		
系统互联情况	☐ 与基础支付系统连接 ☐ 与金融行业其他系统连接 ☐ 与本单位其他系统连接 ☐ 其他		
系统是否具有密码应用方案	☐ 有密码应用方案，且通过密评，密评机构名称： ☐ 有密码应用方案，但未通过密评 ☐ 无密码应用方案		
系统使用的密码产品情况	☐ 系统使用的密码产品（含/不含），独立使用（含/不含），共享使用（含/不含）； 其中，取得认证证书的密码产品数量（含/不含），未取得认证证书的国产密码产品数量（含/不含），国外产品数量（含/不含）。		
系统使用的密码算法	对称算法： ☐ SM1 ☐ SM4 ☐ SM7 ☐ AES ☐ DES ☐ 3DES ☐ 其他 非对称算法： ☐ SM2 ☐ SM9 ☐ RSA1024 ☐ RSA2048 ☐ 其他 杂凑算法： ☐ SM3 ☐ SHA-1 ☐ SHA-256 ☐ SHA-384 ☐ SHA-512 ☐ MD5 ☐ 其他 序列算法： ☐ ZUC ☐ 其他 其他算法：		
密评机构			
单位名称			
通信地址			邮政编码
联系人	姓名	职务/职称	
	所属部门	办公电话	
	移动电话	电子邮箱	

新增

2021版与2023版系统密评模版“总体评价：添加测评结果模版”对比

商用密码应用安全性评估报告模板

2021

总体评价

本次信息系统商用密码应用安全性评估依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第(X)级别要求，选取的测评指标总数为 XXX 项，其中不适用项为 XXX 项，特殊指标 XXX 项，测评结果为：符合项 XXX 项，部分符合项 XXX 项，不符合项 XXX 项，其中：在部分符合和不符合项中：高风险项 XXX 项，中风险项 XXX 项，低风险项 XXX 项。

1. 在物理和环境安全方面，XXX
2. 在网络和通信安全方面，XXX
3. 在设备和计算安全方面，XXX
4. 在应用和数据安全方面，XXX
5. 在管理制度方面，XXX
6. 在人员管理方面，XXX
7. 在建设运行方面，XXX
8. 在应急处置方面，XXX

通过对 XXXXX 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，管理制度，人员管理，建设运行和应急处置等方面的测评，该系统(符合/基本符合/不符合)GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第(X)级别要求。

新增测评结果模版

总体评价

本次信息系统商用密码应用安全性评估依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第(X)级别要求，选取的测评指标总数为 XXX 项，其中不适用项为 XXX 项，特殊指标 XXX 项，测评结果为：符合项 XXX 项，部分符合项 XXX 项，不符合项 XXX 项，其中：在部分符合和不符合项中：高风险项 XXX 项，中风险项 XXX 项，低风险项 XXX 项。

1. 在物理和环境安全方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

2. 在网络和通信安全方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

3. 在设备和计算安全方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

4. 在应用和数据安全方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

5. 在管理制度方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

6. 在人员管理方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

7. 在建设运行方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

8. 在应急处置方面，XXX

测评结果：符合项 XX 项，部分符合项 XX 项，不符合项 XX 项，不适用项 XX 项。

通过对 XXXXX 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，管理制度，人员管理，建设运行和应急处置等方面的测评，该系统(符合/基本符合/不符合)GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第(X)级别要求。

商用密码应用安全性评估报告模板

2023

2021版与2023版系统密评模版“测评准备阶段、物理环境”对比

测评准备阶段

2021年

角色	姓名	任务分工
项目负责人		
测评项目组成员		

2023年

角色	姓名	任务分工	是否通过密评人员考核
项目负责人			
测评项目组成员			

新增

是否通过密评人员考核

物理环境

2021年

表 2-1 物理环境

序号	物理环境名称	物理位置	重要程度
1			
2			

表 2-2 物理安防设施

序号	产品名称	生产厂商和型号	所在物理环境名称	重要程度
1				
2				

新增

物理环境名称示例

2023年

表 2-1 物理环境

序号	物理环境名称	物理位置	重要程度
1	XX 机房		
2	XX 机房		

表 2-2 物理安防设施

序号	产品名称	生产厂商和型号	所在物理环境名称	重要程度
1	电子门禁系统			
2	视频监控系統			

新增

产品名称示例

2021版与2023版系统密评模版“安全威胁、前次测评情况”对比

2021版

2.6 安全威胁

表 2-12 安全威胁

序号	威胁层面	威胁分类
TP1	物理和环境	非法人员进入物理环境，对基础设备和系统运行造成破坏
TP2		物理进出记录和视频监控记录遭到篡改，以掩盖非法人员进出情况
TN1	网络和通信	非法通信实体接入网络
TN2		部分数据在信息系统中被非法授权的截获、篡改
TN3		非法设备从外部接入内部网络，或网络边界被破坏
TD1	设备和计算	设备被非法人员登录
TD2		通过远程管理通道被非法使用，系统内的管理数据被非法获取和篡改
TD3		设备资源被登录设备的其他用户获取
TD4		重要信息受安全标记被非法授权获取和篡改

“威胁层面”修改为
“安全层面”

2023版

2.6 安全威胁

表 2-12 安全威胁

序号	安全层面	威胁分类
TP1	物理和环境	非法人员进入物理环境，对基础设备和系统运行造成破坏
TP2		物理进出记录和视频监控记录遭到篡改，以掩盖非法人员进出情况
TN1	网络和通信	非法通信实体接入网络
TN2		部分数据在信息系统中被非法授权的截获、篡改
TN3		非法设备从外部接入内部网络，或网络边界被破坏
TD1	设备和计算	设备被非法人员登录
TD2		通过远程管理通道被非法使用，系统内的管理数据被非法获取和篡改
TD3		设备资源被登录设备的其他用户获取
TD4		重要信息受安全标记被非法授权获取和篡改

2.7 前次测评情况

本次测评是被测信息系统进行的第____次商用密码应用安全性评估，上次评估时间为____年____月____日，评估结论为：_____。

2.7 前次测评情况

本次测评是被测信息系统进行的第____次商用密码应用安全性评估，上次评估时间为____年____月____日，密评机构为：_____，评估结论为：_____，综合得分为：_____。

2021版

6 风险分析

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					1	0	0
2							
统计							

增加了“安全层面”和“问题描述”的具体示例内容

附录A 测评结构记录

A.1 物理和环境安全

表 A-1 物理和环境安全评价结果记录

[illegible]

“密码使用安全”修改为“密码使用有效性”

2023版

6 风险分析

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	身份鉴别: 通过用户名和密码鉴别用户身份			1	0	0
2		电子门禁记录数据存储完整性: 通过完整性校验码验证数据完整性					
3		视频监控记录数据存储完整性: 通过完整性校验码验证数据完整性					
4		通过完整性校验码验证数据完整性					
合计							

附录A 测评结构记录

A.1 物理和环境安全

表 A-1 物理和环境安全属性评估记录

测评单元	测评对象	结果记录	测评指标				测试单元得分
			密码 使用 合规 性	密码 算法、 技术 合规 性	密码 管理 合规 性	测评 对象 得分	
			$S_{3.1}$	$S_{3.2}$	$S_{3.3}$	$S_{3.4}$	$\frac{S_{3.1}+S_{3.2}+S_{3.3}+S_{3.4}}{4}$

2023版系统密评模版完善了“密评活动有效性证明记录”相关内容

新增

根据密评结果备案审查需求，2023版报告模板增加“附录B密评活动有效性证明记录”，包含**B.1密评委托证明**、**B.2密评活动证明**、**B.3密评活动质量文件**、**B.4密评人员资格证明**、**B.5系统定级匹配证明**

B.1 密评委托证明

表 B-1 密评委托证明			
委托单位	受托单位	委托日期	受托日期
委托事项	受托事项	委托期限	受托期限
委托内容	受托内容	委托地点	受托地点
委托单位（盖章）：_____			
受托单位（盖章）：_____			

B.2 密评活动证明

表 B-2 密评活动证明			
活动名称	活动地点	活动时间	活动人员
活动内容	活动形式	活动结果	活动评价
活动单位（盖章）：_____			

表 B-3 密评活动证明			
活动名称	活动地点	活动时间	活动人员
活动内容	活动形式	活动结果	活动评价
活动单位（盖章）：_____			

B.3 密评活动质量文件

表 B-4 密评活动质量文件	
文件名称	文件内容
文件编号	文件日期
文件单位（盖章）：_____	

表 B-5 密评活动质量文件	
文件名称	文件内容
文件编号	文件日期
文件单位（盖章）：_____	

表 B-6 密评活动质量文件	
文件名称	文件内容
文件编号	文件日期
文件单位（盖章）：_____	

B.4 密评人员资格证明

表 B-7 密评人员资格证明			
序号	姓名	职位	密评人员考核时间
1		[姓名、身份证号等]	2023.01.20-21
2		[姓名、身份证号等]	2023.01.20-21
3		[姓名、身份证号等]	2023.01.20-21
4		[姓名、身份证号等]	2023.01.20-21
5		[姓名、身份证号等]	2023.01.20-21

表 B-8 密评人员资格证明	
姓名	身份证号
姓名	身份证号
姓名	身份证号

B.5 系统定级匹配证明

表 B-9 系统定级匹配证明	
系统名称	系统定级
系统名称	系统定级
系统名称	系统定级

2023版《密评报告模版》之**方案密评报告**模版修改点总览

方案密评模版 六处增加点

基本信息表

- 1 a) **增加**被测系统是否属于关键信息基础设施
- b) **增加**系统依赖情况，即是否依赖不在本系统范围内的云平台运行

2 “商用密码应用安全性评估结论” **增加**方案介绍要求

3 表3指标适用情况及论证说明 “应” 指标**增加** “☐不适用” 选项

4 “5” **增加**方案“报告分发范围”的描述，与系统评估报告保持一致

5 **增加**附录A密评活动有效性证明记录”，主要包含以下内容：

- a) 密评委托证明 b) 密评活动证明 c) 密评活动质量文件 d) 密评人员资格证

基本信息表

[illegible]

新增：“基本信息表”中“信息系统”部分新增“系统是否依赖不在本系统范围内的云平台运行”项。其中，如果云平台正在评估，评估时间和评估结论可以为空。

《XXX系统密码应用方案》密评报告模版“评估结论”、“表3”修订对照

2021版

商用密码应用安全性评估结论	
方案名称	
方案简介	(简述系统情况、方案内容。)

2023版

商用密码应用安全性评估结论	
方案名称	
方案简介	(简述系统情况、主要密码应用措施和密码应用实现内容。)

细化：“商用密码应用安全性评估结论”表格进一步细化方案简介内容描述，要求描述“方案重点解决的系统密码应用需求和密码实现等内容”。

调整：“表3 指标使用情况及论证说明”中应用要求为“应”的，其适用情况全部调整为“☐适用”和“☐不适用”。以下截图为部分内容示例说明。

表 3 指标使用情况及论证说明

安全属性	指标要求	应用要求	适用情况	不适用性论证说明
物理和环境安全	8.1.4) 应采用密码技术进行数据访问与鉴别，保证数据机密、完整和不可否认性。	应	☐ 适用 ☐ 不适用	不适用，对数据不敏感，不涉及密码。
	8.1.5) 应采用密码技术保护电子信息系统安全记录数据的机密性。	应	☐ 适用 ☐ 不适用	
	8.1.6) 应采用密码技术保证数据备份及还原数据的完整性。	应	☐ 适用 ☐ 不适用	
网络和通信安全	8.2.4) 应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。	应	☒ 适用	
	8.2.5) 应采用密码技术保证通信过程中数据的机密性。	应	☐ 适用 ☐ 不适用	
	8.2.6) 应采用密码技术保证通信过程中数据的完整性。	应	☐ 适用 ☐ 不适用	
	8.2.7) 应采用密码技术保证通信过程中数据的不可否认性。	应	☐ 适用 ☐ 不适用	
	8.2.8) 应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。	应	☐ 适用 ☐ 不适用	

表 3 指标使用情况及论证说明

安全属性	指标要求	应用要求	适用情况	不适用性论证说明
物理和环境安全	8.1.4) 应采用密码技术进行数据访问与鉴别，保证数据机密、完整和不可否认性。	应	☐ 适用 ☐ 不适用	不适用，对数据不敏感，不涉及密码。
	8.1.5) 应采用密码技术保护电子信息系统安全记录数据的机密性。	应	☐ 适用 ☐ 不适用	
	8.1.6) 应采用密码技术保证数据备份及还原数据的完整性。	应	☐ 适用 ☐ 不适用	
网络和通信安全	8.2.4) 应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。	应	☒ 适用 ☐ 不适用	
	8.2.5) 应采用密码技术保证通信过程中数据的机密性。	应	☐ 适用 ☐ 不适用	
	8.2.6) 应采用密码技术保证通信过程中数据的完整性。	应	☐ 适用 ☐ 不适用	
	8.2.7) 应采用密码技术保证通信过程中数据的不可否认性。	应	☐ 适用 ☐ 不适用	
	8.2.8) 应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。	应	☐ 适用 ☐ 不适用	

2021版与2023版方案密评模版“报告分发范围、附录A”对比

5 报告分发范围

本报告一式 X 份，其中 X 份提交密码管理部门，X 份提交委托单位，X 份由密评机构留存。

2023版

新增：2023版新增了“5 报告分发范围”部分，要求将报告提交密码管理部门、委托单位和密评机构留存。

新增：新增“附录A 密评活动有效性证明记录”，包含密评委托证明、密评活动证明、密评活动质量文件、密评活动质量文件、系统定级匹配证明等相关文件。

附录 A 密评活动有效性证明记录²

A.1 密评委托证明¹

表 A-1 密评证明文件

文件类型	合同附件一	签订时间	20XX 年 XX 月 XX 日
委托单位			
委托金额	XXXX 元	方案密评单价	XXXX 元
(委托证明扫描件)			

A.2 密评活动证明¹

表 A-2 密评活动证明

方案评估起止时间	20XX 年 XX 月 XX 日-20XX 年 XX 月 XX 日
密评人员	
[活动证明扫描件]	

A.3 密评活动质量文件

表 A-3 密评报告评审

报告评审时间	20XX 年 XX 月 XX 日
[方案评估报告评审记录扫描件]	

A.4 系统定级匹配证明

表 A-4 系统定级备案证明

系统等级定级备案名称	
系统等级定级备案时间	20XX 年 XX 月 XX 日
[信息系统安全等级保护备案证明扫描件]	

A.4 密评人员资格证明¹

表 A-4 密评人员资格情况

序号	姓名	角色	密评人员考试通过时间
1		(组长, 密评报告编制人)	20XX 年 XX 月
2		(顾问)	20XX 年 XX 月
3		(组员)	20XX 年 XX 月
4		(密评报告审核人)	20XX 年 XX 月
5		(密评报告编制人)	20XX 年 XX 月

表 A-5 密评人员考核成绩证明

(或填写扫描件)	(或填写扫描件)
----------	----------

- 01 密评背景介绍
- 02 密评总体要求
- 03 密评测评要求
- 04 密评方案要求
- 05 密评测评过程

06 密评团标解读

- 07 密改FAQ解读
- 08 密改方案实践



《信息系统密码应用方案评估规范》

TGDCCA 0001-2022

统一密码应用方案评估标准，规范实施评估工作

2022年5月19日，广东省商用密码协会发布T/GDCCA 0001—2022《信息系统密码应用方案评估规范》，于2022年6月1日正式实施，旨在：

规定信息系统密码应用方案评估的方法及要点，指导、规范密码应用方案评估方对密码应用方案开展评估工作。



明确4个重要定义和3个缩略语

密码应用方案评估

Evaluation for Cryptography Application Scheme

- 方案评估方对信息系统密码应用方案开展审查，给出建议，并出具相关报告的过程。以下简称“方案评估”。

方案编制方

Organization of Scheme Compilation

- 信息系统密码应用方案编制单位，负责方案的编写和修正工作。

方案评估方

Organization of Scheme Evaluation

- 接受委托单位委托，实施方案评估的机构或团体，包括商用密码安全性评估机构和信息系统责任单位自行或者委托组织的专家组。

密码应用方案评估人员

Evaluator of Cryptography Application Scheme

- 信息系统密码应用方案评估方参与方案评估活动的实施人员。

*GM/Z4001-2013 中界定的以及以上术语和定义适用于本文件。

A

密码算法/技术合规性

(Cryptography **A**lgorithm/Technique compliance)

D

密码使用有效性

(Cryptography **D**eployment effectiveness)

K

密钥管理安全

(**K**ey management security)

规定信息系统密码应用方案评估的5大环节



丰富形式审核和实质审核的结果判定依据

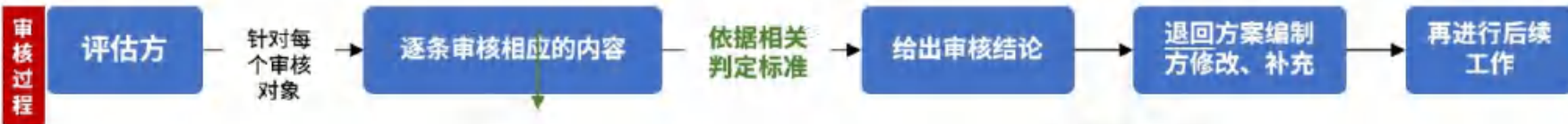
1. 形式审核

2. 实质审核

3. 指标评估

4. 初步量化评估

5. 结论判定



判定标准	形式审核				实质审核			
	结论	判定依据			结论	判定依据		
		方案内容		是否满足评估需要		方案内容		是否满足评估需要
	符合	对应审核 条目	齐备可用	满足	符合	对应审核 条目	正确、有效	满足
	基本符合		- 存在部分缺失， - 存在影响可用性的问题	- 基本满足 - 方案评估人员能针对方案实施评估	基本符合		基本满足条目要求	不影响评估人员实施评估
	不符合		严重缺失或可用性差	方案评估人员无法依据方案有根据地实施评估	不符合		- 缺少必要的审核对象 - 审核对象的内容严重缺失 - 存在严重错误	- 影响评估人员实施评估 - 实施保障措施不合理，导致方案不能正常实施

形式审核侧重内容的完整性、一致性和文本规范性

1. 形式审核

2. 实质审核

3. 指标评估

4. 初步量化评估

5. 结论判定



内容完整性

1. 审核对象：方案文本
2. 审核实施：针对审核对象，对照**附录A**逐条审核以下内容：

R 背景	第1~2项
R 系统概述	第1~9项
R 密码应用需求分析	第1~3项
R 设计目标及原则	第1~2项
R 技术方案	第1~7项
R 安全管理	第1~4项
R 实施保障	

3. 结果判定：审核结果为“符合”“基本符合”“不符合”



内容一致性

1. 审核对象：方案文本
2. 审核实施：针对审核对象，逐条审核以下各条是否一致：

R 密码应用部署网络拓扑图、密码应用安全需求、安全控制措施	
R 密码应用部署网络拓扑图标识的商用密码产品	与系统密码软硬件产品清单
R 密码应用技术框架、密码应用四个安全层面设计	
R 密码应用合规性自查表列出的指标项	
GB/T39786-2021附录A相应密评等级的要求	与密码应用合规性自查表指标适用情况及论证说明
与密码应用场景	
R 密码应用合规性自查表描述的安全控制措施	与密码应用部署网络拓扑图

3. 结果判定：审核结果为“符合”“基本符合”“不符合”



文本规范性

1. 审核对象：方案文本
2. 审核实施：针对审核对象，逐条审核以下内容：

R 文字畅通，不存在影响阅读和理解的漏字、错别字，排版错误等问题；
R 涉及密码应用场景、密码应用需求分析和采取安全控制措施的内容，应表述清晰、无歧义；
R 涉及的密码技术专业术语使用准确。

3. 结果判定：审核结果为“符合”“基本符合”“不符合”

形式审核参考附录A：信息系统密码应用方案编制指引

1.
形式
审核

密码应用方案设计与信息系统业务相结合，与信息系统整体网络安全等级保护相一致，在设计系统总体方案同时，给出密码支撑总体架构设计，引导密码在信息系统中的应用。

2.
实质
审核

采用商用密码产品和服务符合实际情况，满足安全需求，不出现过度保护，增加额外费用。

3.
指标
评估

密码应用方案应该切合实际、合理可行。方案设计要在保证信息系统业务正常运行的同时，综合考虑信息系统的复杂性、兼容性及其他保障措施。

4.
初步
量化
评估

5.
结论
判定



依据GB/T39786-2021，通过成体系、分层次设计，形成包括密码支撑总体架构、密码基础设施建设部署、密钥管理体系构建、密码产品部署及管理等内容。为实现该基本要求在具体信息系统上落地创造条件。

密码应用方案在密码技术应用、密钥管理和安全管理方面均按照相关要求设计，组成完备的密码支撑保障体系

形式审核参考附录A：方案审核要件清单

要件清单（包含但不限于以下内容）	
1. 形式审核	背景 1、应包含系统建设规划概述； 2、应包含项目实施的法律、法规依据及必要性。
2. 实质审核	系统概述 1. 应明确给出当前系统等级定级情况； 2. 应给出系统名称、项目建设单位名称、地址、类型及所属密码管理部门，系统使用单位、使用人员； 3. 应明确具体使用场景，正确给出描述； 4. 应给出信息系统所在机房情况，包括机房的物理位置、管理责任单位及地址，现有的安全防护措施：包括但不限于门禁系统、视频监控系统等； 5. 应给出正确的系统网络拓扑图，并给出相应文字说明。包括网络体系架构、网络区域划分、系统软硬件构成； 6. 应明确网络边界划分，指出连接系统的网络通道； 7. 应给出系统承载的业务应用、业务功能； 8. 应明确系统信息种类、关键数据类型及保护需求，除业务数据外，应包含密钥数据、身份鉴别数据、个人隐私信息； 9. 应明确现有的管理制度。
3. 指标评估	密码应用需求分析 1. 应结合实际具体使用的业务场景，准确给出针对性的系统安全风险分析及控制措施； 2. 应针对安全风险，依据GB/T39786-2021以及应用系统的实际情况，按照系统等保定级，正确给出密码应用安全需求分析，并明确系统各层密码应用保护对象； 3. 对应系统的密评等级，明确各密码应用保护对象是否适用于GB/T39786-2021指标要求的不适用项，如果不适用则应给出原因说明，并给出替代性措施。
4. 初步量化评估	设计目标及原则 1. 应给出总的设计目标或阶段设计目标，且设计目标合理； 2. 应给出总的设计原则，依据的与密码相关的政策法规和技术标准、规范。设计原则合理，给出的技术标准和规范应汇集方案中所有出现的技术标准和规范具体名称。
5. 结论判定	技术方案 1. 对应系统的密评等级，应给出符合GB/T39786-2021对应等级相关要求的技术方案。 2. 应给出密码应用技术框架及文字说明。该技术框架应结合系统应用场景正确、清晰描述设计的密码应用，且仅包含本项目涉及到的密码技术、功能、服务； 3. 应正确给出技术要求四个层面（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）的密码保护对象、采取的密码保护措施（密码算法、密码协议、密码产品、密码服务）及其遵循的标准。 4. 对于密码应用依据标准、规范，但不依赖合规的密码产品/系统设计实现，设计或实现中自主度较大的部分，应给出具体实现的安全机制、工作流程、密钥管理体系与实现。 5. 应正确描述系统中密钥管理方案，该管理方案应结合各（类）密码管理局期进行设计，包含分析密钥种类、属性、层次、生命周期安全等。给出使用的独立的密钥管理设备或设施。 6. 应给出系统密码应用部署拓扑图和系统密码软硬件产品清单。出现在产品清单中的密码软硬件产品应该以图标形式出现在拓扑图中。图示应明确各类用户与通道，结合网络边界划分，能识别出网络安全域（分区）。 7. 应给出密码应用合规性自查表。内容包含采取的密码保护措施及具体算法、技术的名称和产品类型。针对不适用项说明原因及替代性措施。
	安全管理方案 1. 应设计管理制度，建立操作规范 2. 应设计人员管理方案，建立相关制度 3. 应设计建设运行方案 4. 应设计应急处置方案
	实施保障方案 应制定实施保障方案，包含以下内容：人员组织保障、实施技术保障、项目质量保障、项目经费保障

实质审核内容以各安全层面的控制点为抓手突出可行性

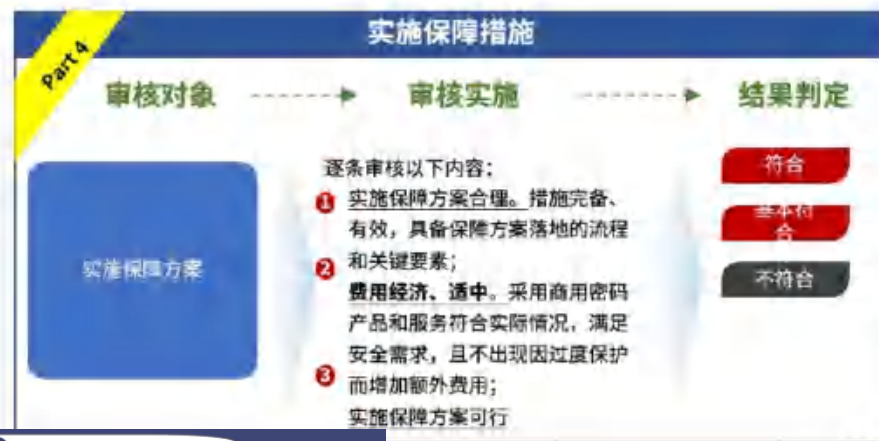
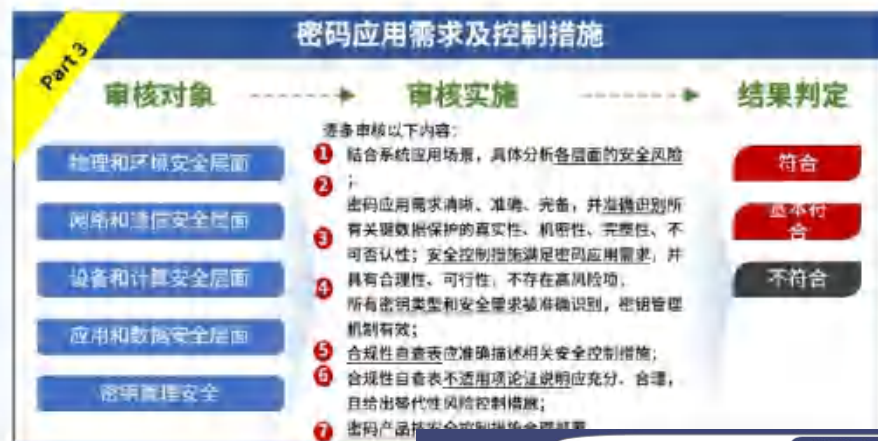
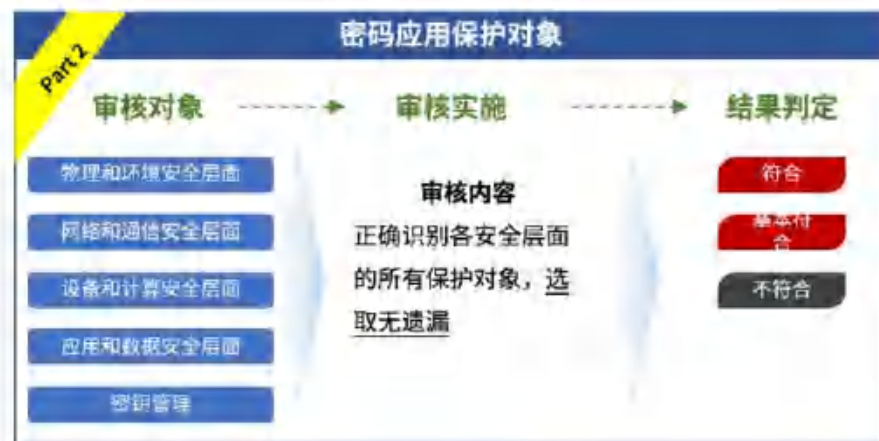
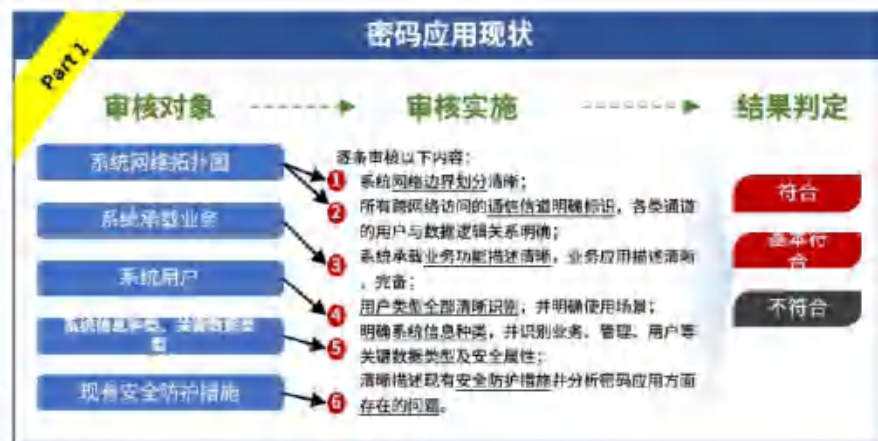
1. 形式审核

2. 实质审核

3. 指标评估

4. 初步量化评估

5. 结论判定



高风险项审核参考附录B

1.
形式
审核

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

审核对象	高风险项
密码算法	MD5
	DES
	SHA-1
	RSA(不足2048)
	RC4
	自行设计的密码算法(安全性未知)
密码技术	经认证的密码产品中未经安全性论证的密码算法
	SSH1.0
	SSL2.0
	SSL3.0
	TLS1.0
	自行设计未经安全论证的密码通信协议
密码产品和密码服务	经认证的密码产品中未经安全性论证的密码通信协议
	采用自实现未提供安全性证据的密码产品
	存在Heartbleed漏洞的OpenSSL产品
	密码服务供应商不具备相关资质
密钥管理	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)
	密钥产生
	密钥分发
	密钥存储
	密钥使用
	密钥更新
	密钥销毁和撤消
	密钥恢复

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

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

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} (2^{40})

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技术关联,但使用前未验证公钥有效性或验证机制不完善
5)未按密钥用途正确使用

未建立密钥已泄露或存在泄露风险时的密钥更新机制

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

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

指标评估方法对标GB/T 39786强调技术评估和管理评估

1.
形式
审核

依据方案给出的信息系统等保定级，确定密评等级，对应GB/T39786-2021的指标实施评估，按技术评估和管理评估划分的评估单元，各单元对应一组相对独立和完整的评估内容

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

技术评估

评估项	内容
保护对象	<u>GB/T39786-2021</u> 中密码应用 <u>技术要求</u> 维度涉及的保护对象
评估对象	相关配套密码产品、通用设备、人员、管理制度文档、建设运行文档、应急处置文档等
评估指标	<u>GB/T39786-2021</u> 中对密码应用 <u>技术要求的指标</u>
评估实施	针对某个评估对象，规定信息系统密码应用方案的 <u>指标评估要点</u>
结果判定	- 根据评估核查证据，判定是否满足某个测评指标要求的方法/原则 判定结论为：通过、不通过

管理评估

评估项	内容
评估对象	相关配套密码产品、通用设备、人员、管理制度文档、建设运行文档、应急处置文档等
评估实施	针对某个评估对象，规定了信息系统密码应用方案的 <u>指标评估要点</u>
结果判定	- 根据评估核查证据，判定是否满足某个测评指标要求的方法/原则 判定结论为：通过、不通过

结果判定说明：

- 若评估单元包含2个及以上评估对象，每个评估对象需分别进行评估、判定结果。评估单元的结果由该单元包含的所有评估对象的评估实施结果汇总得出。
- 当评估单元中所有评估对象评估结论为“通过”，则该评估单元评估结论为“通过”；如果评估单元中所有评估对象，则该评估单元评估结论为“不通过”。

GB/T39786-2021技术和管理要求维度涉及的保护对象

1.
形式
审核

技术要求

技术要求主要由机密性、完整性、真实性、不可否认性4个密码安全功能维度构成，具体保护对象或应用场景描述如下：

机密性技术要求保护对象

使用密码技术的加解密功能实现机密性

- 身份鉴别信息
- 密钥数据
- 传输的重要数据
- 信息系统应用中所有存储的重要数据

完整性技术要求保护对象

使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现完整性

- 身份鉴别信息
- 密钥数据
- 日志记录
- 访问控制信息
- 重要信息资源安全标记
- 重要可执行程序
- 视频监控音像记录
- 电子门禁系统进出记录
- 传输的重要数据
- 信息系统应用中所有存储的重要数据

真实性技术要求应用场景

使用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现真实性

- 进入重要物理区域人员的身份鉴别
- 通信双方的身份鉴别
- 网络设备接入时的身份鉴别
- 重要可执行程序的来源真实性保证
- 登录操作系统和数据库系统的用户身份鉴别
- 应用系统的用户身份鉴别

不可否认性技术要求 保护对象

使用基于公钥密码算法的数字签名机制等密码技术来保证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。

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

管理要求

管理要求由管理制度、人员管理、建设运行、应急处置等4个密码应用管理维度构成，具体如下：

管理制度

密码应用安全管理相关流程制度的制定、发布、修订的规范性要求

人员管理

密码相关安全人员的密码安全意识以及关键密码安全岗位员工的密码安全能力的培训、人员工作流程要求等

建设运行

建设运行过程中密码应用安全要求及方案落地执行的一致性和有效性要求

应急处置

处理密码应用安全相关的应急突发事件的能力要求

1. 形式审核

物理和环境安全-指标体系	一级	二级	三级	四级
身份鉴别	可	宜	宜	应
电子门禁记录数据存储完整性	可	可	宜	应
视频监控记录数据存储完整性	—	—	宜	应
密码产品	—	应一级	应二级	应三级
密码服务	应	应	应	应

2. 实质审核

3. 指标评估

设备和计算安全-指标体系	一级	二级	三级	四级
身份鉴别	可	宜	应	应
日志记录完整性	可	可	宜	应
远程管理通道安全	—	—	应	应
系统资源访问控制信息完整性	可	可	宜	应
重要可执行程序完整性、重要可执行程序来源真实性	—	—	宜	应
重要信息资源安全标记完整性	—	—	宜	应
密码产品	—	应一级	应二级	应三级
密码服务	应	应	应	应

4. 初步量化评估

5. 结论判定

网络和通信安全-指标体系	一级	二级	三级	四级
身份鉴别	可	宜	应	应
通信数据完整性	可	可	宜	应
通信过程中重要数据的机密性	可	宜	应	应
网络边界访问控制信息的完整性	可	可	宜	应
密码产品	—	应一级	应二级	应三级
安全接入认证	—	—	可	宜
密码服务	应	应	应	应

应用和数据安全-指标体系	一级	二级	三级	四级
身份鉴别	可	宜	应	应
重要数据传输机密性	可	宜	应	应
重要数据传输完整性	可	宜	宜	应
重要数据存储机密性	可	宜	应	应
重要数据存储完整性	可	宜	宜	应
访问控制信息完整性	可	可	宜	应
密码产品	—	应一级	应二级	应三级
不可否认性	—	—	宜	应
密码服务	应	应	应	应
重要信息资源安全标记完整性	—	—	宜	应

GB/T39786-2021管理评估指标

1.
形式
审核

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

管理制度-指标体系	一级	二级	三级	四级
具备密码应用安全管理制度	应	应	应	应
定期修订安全管理制度	—	—	应	应
明确管理制度发布流程	—	—	应	应
制度执行过程记录留存	—	—	应	应
密钥管理规则	应	应	应	应
建立操作规程	—	应	应	应

建设运行-指标体系	一级	二级	三级	四级
制定密码应用方案	应	应	应	应
制定密钥安全管理策略	应	应	应	应
制定实施方案	应	应	应	应
投入运行前进行密码应用安全性评估	可	宜	应	应
定期开展密码应用安全性评估及攻防对抗演习	—	—	应	应

人员管理-指标体系	一级	二级	三级	四级
了解并遵守密码相关法律法规和密码管理制度	应	应	应	应
建立上岗人员培训制度	—	应	应	应
建立密码应用岗位责任制度	—	应	应	应
建立关键岗位人员保密制度和调离制度	应	应	应	应
定期进行安全岗位人员考核	—	—	应	应

应急处置-指标体系	一级	二级	三级	四级
应急策略	可	应	应	应
事件处置	-	-	应	应
向有关主管部门上报处置情况	-	-	应	应

技术评估之身份鉴别

1.
形式
审核

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

安全层面	保护对象	评估对象	评估指标	评估实施	结果判定
物理和环境	物理机房	信息系统所在机房等重要区域及其电子门禁系统	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（第一到第四级）		
网络和通信	通信信道	提供通信信道身份鉴别功能的密码设备、组件 提供网络通信设备入网接入认证功能的密码设备、组件	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）3) 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（第三到第四级）	针对所运用的评估对象，逐项核查评估以下内容： 1) 审核是否满足密码算法和技术的合规性 2) 审核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进行身份鉴别 3) 审核真实性实现机制是否正确、有效 4) 若采取了缓解替代性风险控制措施，审核其措施是否能够有效控制风险	针对单个评估对象，按照如下规则判定结果： 1) <u>未采用密码技术或采用了“高风险”密码算法、密码技术、密码产品和密码服务实现身份鉴别，而且采取的安全控制措施无法缓解“高风险”，或者无法满足系统的安全需求，则评估结论为“不通过”</u> 2) <u>采用了非“高风险”密码算法、密码技术、密码产品、密码服务实现身份鉴别，但是方案中描述的实施保障措施不合理，方案无法实施，则评估结论为“不通过”</u> 3) 如果未出现 1)或2)的情况，则评估结论为“通过”
设备和计算	堡垒机、应用服务器、数据库服务器、数据库管理系统等设备和系统，服务器密码机等整机类密码产品，电子签章系统等系统类密码产品	为堡垒机、应用服务器、数据库服务器、数据库管理系统提供身份鉴别功能的密码设备、组件 整机类密码产品的身份鉴别组件；系统类密码产品的身份鉴别组件	1) 采用密码技术对登录设备的用户进行身份鉴别， <u>保证用户身份的真实性（第一到第四级）</u> 2) 远程管理设备时，采用密码技术建立安全的信息传输通道，进行身份鉴别，保证管理设备用户身份的真实性（第三到第四级） 3) 采用密码技术对重要可执行程序来源进行真实性验证（第三到第四级）		
应用和数据	应用用户	为业务应用的用户提供身份鉴别功能的密码设备、组件	采用密码技术对登录用户进行身份鉴别， <u>保证应用系统用户身份的真实性（第一到第四级）</u>		

技术评估信息安全三属性之机密性

1.
形式
审核

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

安全层面	保护对象	评估对象	评估指标	评估实施	结果判定
网络和通信	通信信道传输的重要数据	信息系统与网络边界外建立的网络通信信道，提供通信信道机密性保护功能的密码设备、组件	采用密码技术保证通信过程中重要数据的机密性（第一到第四级）	针对所适用的评估对象，逐项核查评估以下内容： 1)审核是否满足密码算法和技术的合规性 2)审核是否采用密码技术的加密解密功能对重要数据在传输或存储过程中进行机密性保护	针对单个评估对象，按照如下规则判定结果： 1) 未采用密码技术或采用了“高风险”密码算法、密码技术、密码产品、密码服务实现机密性保护，而且采取的安全控制措施无法缓解“高风险”，或者无法满足系统的安全需求，则评估结论为“不通过” 2)采用了非“高风险”密码算法、密码技术、密码产品、密码服务实现机密性保护，但是方案中描述的实施保障措施不合理，方案无法实施，则评估结论为“不通过” 3)如果出现1)或2)的情况，则评估结论为“通过”
		提供远程管理通道的网络设备、组件，密码设备、组件	远程管理设备时，采用密码技术建立安全的信息传输通道，提供传输数据机密性保护（第三到第四级）	3)审核机密性保护机制是否正确、有效 4)若采取了缓解替代性风险控制措施，审核其措施是否能够有效控制风险	
设备和计算	远程管理通道传输的重要数据				
应用和数据	业务应用传输的重要数据、业务应用存储的重要数据	业务应用以及为业务应用的用户提供机密性保护功能的密码设备、组件	采用密码技术保证信息系统应用的重要数据在传输、存储过程中的机密性（第一到第四级）		

技术评估信息安全三属性之完整性



1. 形式审核

2. 实质审核

3. 指标评估

4. 初步量化评估

5. 结论判定

安全层面	保护对象	评估对象	评估指标	评估实施	结果判定
物理和环境	门禁记录数据、视频监控记录	信息系统所在机房等重要区域及其电子设备、门禁系统	1) 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) 2) 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)		
网络和通信	经通信信道传输的重要数据、网络边界访问控制信息	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	采用密码技术保证通信过程中数据和网络边界访问控制信息的完整性(第一到四级)		针对单个评估对象, 按照如下规则判定结果: 1) 未采用密码技术或采用
设备和计算	系统资源访问控制信息、重要信息资源安全标记、日志记录、重要可执行程序	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	1) 远程管理设备时, 采用密码技术建立安全的信息传输通道, 提供传输数据完整性保护(第三级到第四级) 2) 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) 3) 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) 4) 采用密码技术保证日志记录的完整性(第一级到第四级) 5) 采用密码技术对重要可执行程序进行完整性保护(第三级到第四级)	针对所适用的评估对象, 逐项核查了“高风险”密码算法、密码技术、密码产品、密码服务实现完整性保护, 合规性而且采取的安全控制措施 1) 审核是否满足密码算法和技术的密码服务实现完整性保护, 合规性而且采取的安全控制措施 2) 审核是否采用基于对称密码算法无法缓解“高风险”, 或或密码杂凑算法的消息鉴别码(MAC)者无法满足系统的安全需求机制、基于公钥密码算法的数字签名, 则评估结论为“不通过” 完整性保护 2) 采用了非“高风险”密码产品、密码服务实现完整性 3) 审核完整性保护机制是否正确和码算法、密码技术、密码有效 4) 若采取了缓解替代性风险控制措施性保护, 但是方案中描述	
应用和数据	访问控制信息、重要信息资源安全标记、业务应用传输的重要数据、业务应用存储的重要数据	业务应用, 以及为业务应用提供完整性保护功能的密码产品	1) 采用密码技术保证信息系统应用的访问控制信息完整性(第一级到第四级) 2) 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) 3) 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) 4) 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	实施, 审核其措施是否能够有效控制 风险 方案无法实施, 则评估结论为“不通过”; 3) 如果未出现 1) 或 2) 的情况, 则评估结论为“通过”	

技术评估信息安全三属性之不可否认性



1.
形式
审核

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

安全层面	保护对象	评估对象	评估指标	评估实施	结果判定
应用和数据	业务应用, 以及为业 可能涉及法律责 任认定的重要操 作行为	务应用的用户提供不 可否认性功能的密码 产品	在可能涉及法律责任 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)	针对单个评估对象, 按照如下规则判定结 针对所适用的评估对象, 逐项核查评估以 下内容: 1)审核是否满足密码算法、技术和密码服 务的合规性 2)审核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 3)审核不可否认性实现机制是否正确和有 效; 4)若采取了缓解替代性风险控制措施, 审 核其措施是否能够有效控制风险	1)未采用基于公钥密码算法的数字签名机 制等密码技术、密码产品和密码服务或者 采用了具有“高风险的”基于公钥密码算 法和密码服务, 而且采取的安全控制措施无 法缓解“高风险”, 或者无法满足系统的 安全需求, 则评估结论为“不通过” 2) 采用了非“高风险”密码算法、密码技 术、密码产品、密码服务, 但是方案中描 述的实施保障措施不合理, 方案无法实施, 则评估结论为“不通过” 3)如果未出现1) 或2)的情况, 则评估结论 为“通过”

技术评估之密钥管理

1. 形式审核

2. 实质审核

3. 指标评估

4. 初步量化评估

5. 结论判定

安全层面	保护对象	评估对象	评估指标	评估实施	结果判定
物理和环境	信息系统所在物理机房门禁系统身份鉴别	机房电子门禁系统身份鉴别密钥管理机制、进出记录的数			
	所涉及的密钥	据完整性保护的密钥管理机制、视频监控系统的密钥管理			
网络和通信	电子门禁记录数据完整性保护、视频监控	机制相应的密码产品、密码服务以及密码算法实现和密码			
	记录数据完整性保护所涉及的密钥	技术实现			
设备和计算	提供通信信道机密性保护、完整性保护以	提供通信信道机密性保护、完整性保护以及身份鉴别			
	及身份鉴别功能密码设备所涉及的密钥	功能密码设备的密钥管理机制			
应用和数据	提供网络通信设备入网接入认证功能的密	提供网络通信设备入网接入认证功能的密码设备、组			
	码设备、组件所涉及的密钥	件的密钥管理机制			
应用和数据	为应用服务器、数据库服务器、数据库管	相应的密码产品、密码服务以及密码算法实现和密码			
	理系统提供机密性保护、完整性保护以及	技术实现			
应用和数据	身份鉴别功能的密码设备、组件所涉及的	为应用服务器、数据库服务器、数据库管理系统提供			
	密钥	机密性保护、完整性保护以及身份鉴别功能的密码设			
应用和数据	为系统类密码产品提供机密性保护、完整	备、组件的密钥管理机制、整机类型密码产品提供机密			
	性保护以及身份鉴别组件所涉及的密钥	性保护、完整性保护以及身份鉴别组件的密钥管理机			
应用和数据	为系统类密码产品提供机密性保护、完整	制			
	性保护以及身份鉴别密码设备、组件所涉	系统类密码产品提供机密性保护、完整性保护以及身			
应用和数据	及的密钥	份鉴别组件的密钥管理机制			
		相应的密码产品、密码服务以及密码算法实现和密码			
应用和数据	为业务应用的用户提供身份鉴别功能的密	应用系统的密钥体系，密钥功能划分。为业务应用的			
	码设备、组件所涉及的密钥。为业务应用数据提供	用户提供服务身份鉴别功能的密码设备、组件的密钥管			
应用和数据	机密性保护、完整性保护密码设备、组件所涉	理机制			
	及的密钥。为业务用户提供服务行为不可否认	为业务应用数据提供机密性保护、完整性保护的密码			
应用和数据	性的密码设备、组件所涉及的密钥	设备、组件的密钥管理机制。为业务用户提供操作行			
		为不可否认性的密码设备、组件的密钥管理机制。			
应用和数据		相应的密码产品、密码服务以及密码算法实现和密码			

- 1) 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)
- 2) 采用的密码产品，达到GB/T 37092 一级及以上安全要求 (第二级)
- 3) 采用的密码产品，达到GB/T 37092 二级及以上安全要求 (第三级)
- 4) 采用的密码产品，达到GB/T 37092 三级及以上安全要求 (第四级)
- 5) 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)

针对所适用的评估对象，逐项核查评估以下内容：

- 1) 审核是否满足密码产品和服务的合规性
- 2) 核查密钥应用安全管理的密码算法、密钥技术实现设计是否正确、有效
- 3) 核查方案给出的密钥体系中的密钥(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

针对单个评估对象，按照如下规则判定结果：

- 1) 密钥管理机制出现高风险项，或者无法满足系统的安全需求，则评估结论为“不通过”
- 2) 密钥管理机制未出现高风险项，但是方案中描述的保障措施不合理，方案无法实施，则评估结论为“不通过”
- 3) 如果未出现1)或2)的情况，则评估结论为“通过”

管理评估

1.
形式
审核

2.
实质
审核

3.
指标
评估

4.
初步
量化
评估

5.
结论
判定

A 管理制度

评估实施

针对评估对象，逐项核查评估以下内容：

- 1) 管理制度章节应包含密码应用安全管理制度或已明确相关要求(第一级到第四级)
- 2) 管理制度章节应包含密钥管理规则(第一级到第四级)
- 3) 管理制度章节应包含建立操作规程(第二级到第四级)
- 4) 管理制度章节应包含定期修订安全管理制度(第三级到第四级)
- 5) 管理制度章节应包含明确管理制度发布流程(第三级到第四级)

B 人员管理

评估实施

针对评估对象，逐项核查评估以下内容：

- 1) 人员管理章节应包含密码管理制度(第一级到第四级)
- 2) 人员管理章节应包含密码应用岗位责任制度(第二级到第四级)
- 3) 人员管理章节应包含上岗人员培训制度(第二级到第四级)
- 4) 人员管理章节应包含安全岗位人员考核制度(第三级到第四级)
- 5) 人员管理章节应包含关键岗位人员保密制度和调离制度(第一级到第四级)

C 建设运行

评估实施

针对评估对象，逐项核查评估以下内容：

- 1) 建设运行章节应包含密钥安全管理策略(第一级到第四级)
- 2) 建设运行章节应包含制定实施方案(第一级到第四级)
- 3) 建设运行章节应要求投入运行前进行密码应用安全性评估(第一级到第二级)
- 4) 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)
- 5) 建设运行章节应要求定期开展密码应用安全性评估及攻防对抗演习(第三级到第四级)

D 应急处置

评估实施

针对评估对象，逐项核查评估以下内容：

- 1) 应急处置章节应包含密码应用应急策略(第二级到第四级)
- 2) 应急处置章节应包含信息系统密码安全事件应急处置办法(第三级到第四级)
- 3) 应急处置办法应包含事件发生后，及时向信息系统主管部门进行报告的要求；(第三级到第四级)
- 4) 应急处置办法应包含事件处置完成后,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的要求(第三级到第四级)

结果判定

如果管理制度章节均已覆盖以上评估要点，便于密码应用方案的实施且无安全管理漏洞，则对该对象实施评估结论为“通过”，否则为“不通过”

更新初步量化评估方法，侧重规范性和可用性

在《商用密码应用安全性评估量化评估规则》基础上，给出初步量化评估方法

1. 形式审核

2. 实质审核

3. 指标评估

4. 初步量化评估

5. 结论判定



《商用密码应用安全性评估量化评估规则》DAK模型

密码使用安全
(D)

密码技术是否被正确、有效使用，以满足信息系统的安全需求，有效提供机密性、完整性、真实性和不可否认性的保护。

密码算法 / 技术安全
(A)

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。密码技术是否遵循密码相关国家标准和行业标准或经国家密码管理局批准。

密钥管理安全
(K)

密钥管理的全生命周期是否安全，用于密码计算或密码管理的密码产品/密码服务是否



内容部分修改



内容保持不变

各测评对象的测评结果量化评估规则

各测评对象量化评估规则中，按照以下办法确定D、A、K，计算S_{i,j,k}的取值方式不变：密码算法/技术的合规性A与《商用密码应用安全性评估量化评估规则》中的要求保持不变；

评估密码应用设计的正确性

替代

评估密码使用的有效性D

评估密码算法和密钥管理机制

替代

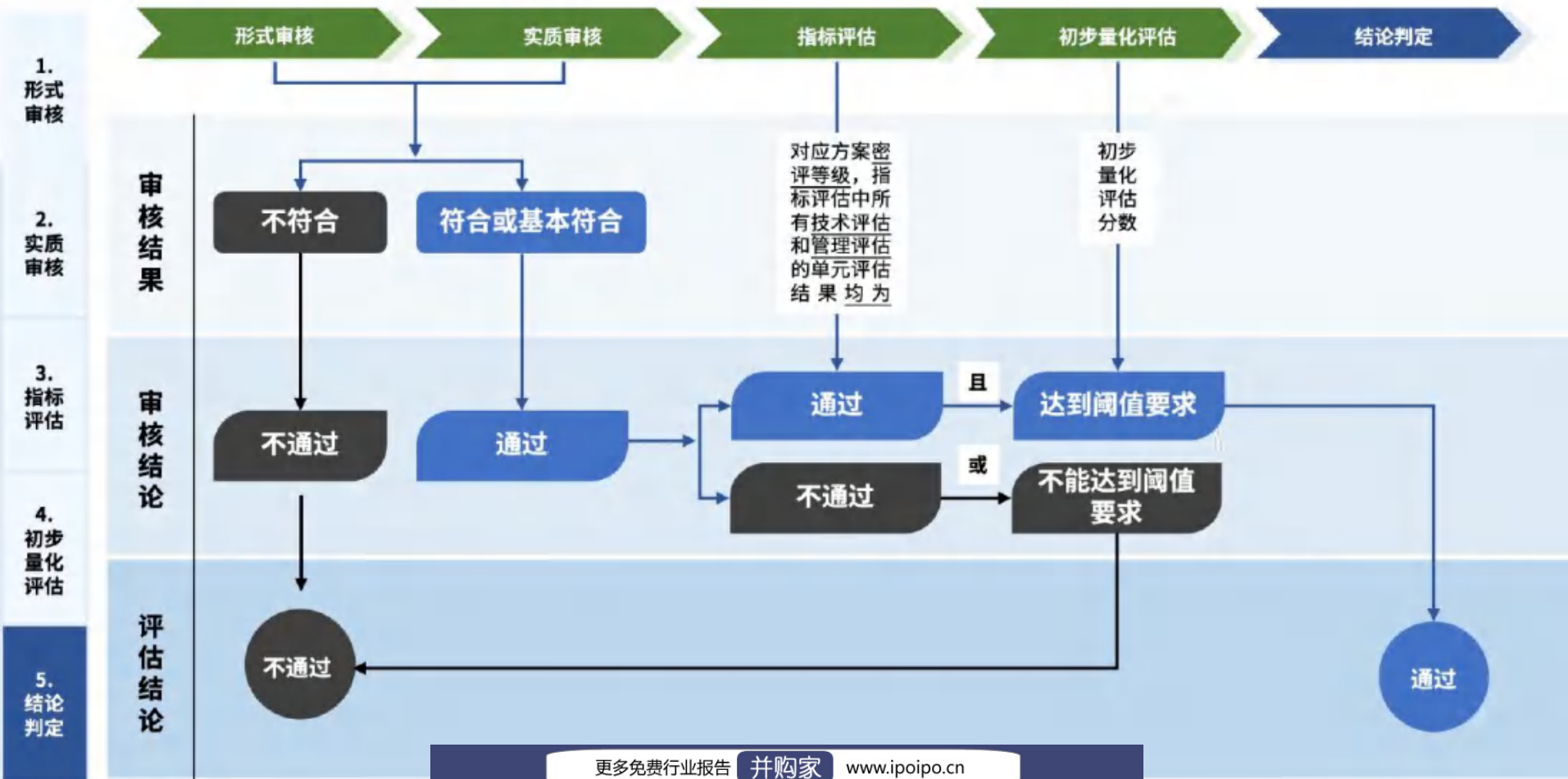
评估密钥管理安全K

测评单元的测评结果量化评估规则

安全层面的测评结果量化评估规则

整体测评结果量化评估规则

明确细化评估结论的判定规则



《信息系统密码应用方案评估过程指南》

TGDCCA 0002-2022

规范密码应用方案评估流程和活动，具有兼容性和指导性作用

2022年5月19日，广东省商用密码协会发布T/GDCCA 0002—2022《信息系统密码应用方案评估过程指南》，并于2022年6月1日正式实施。



明确了五大重要定义

密码应用方案评估

Evaluation for Cryptography Application Scheme

方案评估方对信息系统密码应用方案开展审查，给出建议，并出具相关报告的过程。以下简称“方案评估”。

1

委托单位

Entrust Organization

委托方案评估方开展方案评估的单位。

2

方案评估方

Organization of Scheme Evaluation

接受委托单位委托，实施方案评估的机构或团体，包括商用密码安全性评估机构和信息系统责任单位自行或者委托组织的专家组。

3

密码应用方案评估人员

Evaluator of Cryptography Application Scheme

方案评估方实施方案评估活动时的实施人员或专家，简称“评估人员”。

4

方案编制方

Organization of Scheme Compilation

信息系统密码应用方案编制单位，负责方案的编写和修正工作。

5

* GM/Z 4001-2013界定的以及以上的术语和定义适用本文件

遵循两大基本原则，细化两类方案评估方具体要求

1. 总体要求

基本原则

客观公正性原则

方案评估过程中，评估人员应保证在符合国家密码主管部门要求及最小主观判断情形下，按照委托单位提供的方案，基于明确定义的评估方式和解释，进行方案评估活动。

结果完善性原则

在正确理解 GB/T 39786-2021 以及各个规范应用文件的基础上，方案评估所产生的结果应客观反映信息系统的密码应用需求。方案评估过程和结果应基于正确的评估方法，以确保其满足要求。

2. 评估准备

3. 评估修正

方案评估方要求

信息泄漏风险规避

附录A-方案评估方要求

4. 安全性审查

5. 报告编制

6. 方案变更评估

方案评估方类型	要求
评估机构	a) 国家密码管理部门认定的商用密码应用安全性评估机构； b) 注册地在广东省，或在广东省设立的分支机构； c) 具有开展方案评估工作所需的办公场所，提供在广东省办公场所租赁或所有权证明材料； d) 在广东省派驻评估人员，提供本地评估人员名单及其社保缴存记录；e) 评估人员应通过国家密码管理部门认可的密评技能培训。
评估专家组	a) 专家组应由三名及以上专家组成； b) 专家组成员应为密码行业、信息安全行业从业人员或者相关领域学者； c) 专家组成员应熟悉GB/T 39786-2021等相关标准； d) 专家组成员应具有高级职称（或相当技术水平），或通过国家密码管理部门认可的密评技能培训。

评估中的风险

系统信息
泄露

委托单位
信息泄露

方案评估方应签署**保密协议**
约束信息泄露风险责任

方案评估分为整体评估和变更评估两种类型

方案评估过程

1. 总体要求

2. 评估准备

3. 评估修正

4. 安全性审查

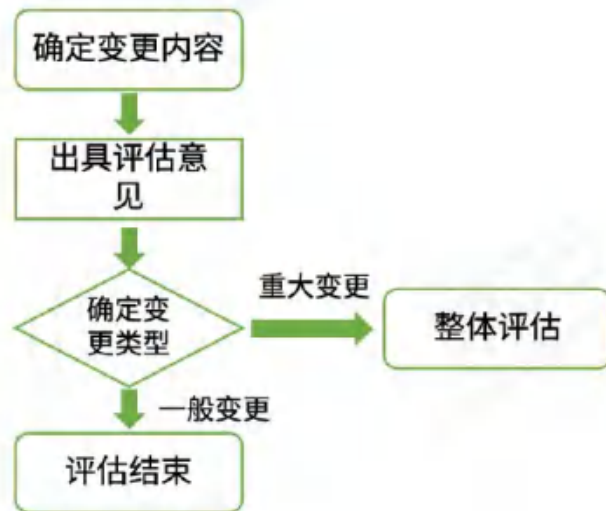
5. 报告编制

6. 方案变更评估

1 整体评估



2 变更评估



评估准备包括项目启动、信息收集两项主要任务

1. 总体要求

2. 评估准备

3. 评估修正

4. 安全性审查

5. 报告编制

6. 方案变更评估



工作内容

- 评估人员与委托单位举行沟通会议，讲解评估过程
- 明确必要项目信息，收集有关项目资料
- 评估准备包括项目启动、信息收集两项主要任务



主要任务

输入

项目启动

委托书或协议书等

任务描述

- 评估人员、方案编制方、委托单位组建项目组。
- 根据委托单位或者方案编制方提供信息系统的基本资料，确定评估计划。

输出

评估计划

信息收集

《系统基本信息表》模板（见附录B）

- 评估人员将《系统基本信息表》模板提供给委托单位、方案编制方。
- 委托单位、方案编制方根据《系统基本信息表》模板提供评估所需资料。
- 评估人员收回填写完成的《系统基本信息表》，与委托单位、方案编制方确认表格信息的正确性和完整性。（注：相关信息将体现到方案密评报告中。）

《系统基本信息表》



报告编制
输入输出物

任务	输入文档	输出文档	输出文档内容
项目启动	委托书或者协议书	评估计划	时间、人员安排等
信息收集	《系统基本信息表》 模板	《系统基本信息表》	单位地址基本信息、相关负责人基本信息、系统名称、方案名称、网络安全等级保护定级情况、备案号、密码应用方案等

附录B-系统基本信息表（模板）

1.总体要求

2.评估准备

3.评估修正

4.安全性审查

5.报告编制

6.方案变更评估

责任单位			
单位名称			
单位地址	邮政编码		
所属省部密码管理部门	广东省密码管理局		
联系人	姓名	职务/职称	
	所属部门	办公电话	
	移动电话	电子邮件	
信息系统			
系统名称			
方案名称			
系统简介			
网络安全等级保护定级情况	已定级，第__级（一至四），S__A__G__。 未定级，本次密评依据GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》第__级（一至四）信息系统要		
网络安全等级保护定级备案情况	已备案 备案证明编号：_____ 未备案	本次被评信息系统与等级保护定级系统是否一致	是 否，变化情况说明：_____ _____
网络安全等级保护测评情况	已测评 测评机构名称：_____ 测评时间：_____ 测评结论：_____ 正在测评 测评机构名称：_____ _____	商用密码应用安全性评估情况	已评估 密评机构名称：_____ 评估时间：_____ 评估结论：_____ 正在评估 密评机构名称：_____ 未评估

评估修正包括评估方案、修正方案和确认方案三项主要任务

1. 总体要求

2. 评估准备

3. 评估修正

4. 安全性审查

5. 报告编制

6. 方案变更评估



工作内容

- 评估人员对密码应用方案进行评估，并将评估后发现的问题和整改建议汇总反馈给方案编制方。
- 方案编制方修改完成后，提交给评估人员。若修改后的方案仍然存在问题，则重复评估修正活动，直到确认方案无误。
- 评估修正包括评估方案、修正方案和确认方案三项主要任务。



主要任务

输入

任务描述

输出

评估方案

密码应用方案

评估人员参照T/GDCCA 0001-2022对密码应用方案展开形式审核、实质审核、技术和管理评估、初步量化等评估活动，审查方案内容的合理性、一致性、可行性、经济性等，分析密码应用正确性、合规性、有效性，以及是否具备完善密码管理制度，按照评估项问题严重程度分级，在将《问题记录表》（见附录C）填写相关问题描述和整改建议，并提交给方案编制方。

《问题记录表》

修正方案

密码应用方案、《问题记录表》

- 方案编制方按照整改建议进行修正，将修正后的密码应用方案重新提交给评估人员再次评估。
- 评估人员对修正后的密码应用方案进行审查，若密码应用方案仍然存在问题，宜重复评估方案和修正方案这两个任务。

修正的密码应用方案

确认方案

修正的密码应用方案

- 评估人员、方案编制方应与委托单位对方案进行确认。
- 如委托单位对方案提出修改要求，则评估人员和方案编写方重复评估方案和修正方案两个任务。
- 方案编制方应将委托单位最终确认的密码应用方案移交给评估人员。

确认后的密码应用方案



输入输出物

任务	输入文档	输出文档	输出文档内容
评估方案	密码应用方案	《问题记录表》	密码应用方案存在问题的所在位置、问题描述、问题级别、整改建议等
修正方案	《问题记录表》	修正的密码应用方案	整改后的密码应用方案内容
确认方案	修正的密码应用方案	确认后的密码应用方案	确认后的密码应用方案内容

附录C-问题记录表

1.总体要求

2.评估准备

3.评估修正

4.安全性审查

5.报告编制

6.方案变更评估

问题级别分类

文法问题

存在语法、文字、格式错误等方面问题

一般问题

非关键内容缺失或描述不完整，系统设计上存在影响整个系统安全性的问题

严重问题

关键内容缺失或描述不完整，系统设计上存在严重影响整个系统安全性的问题，或密码使用上存在合规性、正确性、有效性的问题；

问题记录表

版本号	方案中问题的所在位置	问题描述	问题级别	整改建议

因特殊原因导致安全评估无法进行时宜启用安全性审查

1. 总体要求



宜启用安全性审查的条件：如果方案中使用了包含非标准算法、协议的未经认证产品或服务而导致无法评估时

2. 评估准备

3. 评估修正

4. 安全性审查

5. 报告编制

6. 方案变更评估



信息系统密码应用方案评估过程指南（T/GDCCA 0002-2022）-安全性审查



《安全性评估报告》编制工作需要反复审核确认

1. 总体要求

信息系统密码应用测评过程指南 (GM/T 0116-2021) - 评测过程-密评报告编制流程

密评报告形成

提出改进建议

进行内部评审

提交被测单位

2. 评估准备



报告编制的流程基本一致

3. 评估修正

信息系统密码应用方案评估过程指南 (T/GDCCA 0002-2022) - 报告编制流程

工作内容分类

编写报告

a) 对方案初步量化评分，对措施进行风险分析，得出评估结论；
b) 依据《商用密码应用安全性评估报告模板(2021版)-方案密评报告》编写报告内容，输出方案评估报告

确认报告

a) 提交方案评估报告给委托单位；
b) 委托单位对方案评估报告进行确认；
c) 输出确认后的方案评估报告

审核报告

a) 评估方进行内部审核，并给出审核意见；
b) 审核不通过，则继续修改报告并修正；
c) 审核通过后，评估人员出具方案评估报告

输出报告

a) 根据要求制作多承载形式及数量的方案评估报告；
b) 评估人员对评估报告签字确认/评估机构盖章；
c) 评估方将正式的报告提交给委托单位

4. 安全性审查

5. 报告编制

6. 方案变更评估

报告编制任务的不同阶段需要输入输出不同文档

1.总体要求

任务

输入文档

输出文档

输出文档内容

2.评估准备

编写报告

《系统基本信息表》、
《问题记录表》、安全性
审查意见（可选）、密码
应用方案

初步的方案评估报告

系统基本信息、密码应用
需求、概述密码应用措施、
指标适用性情况、问题整
改情况、评估结论等

3.评估修正

确认报告

初步的方案评估报告

委托单位确认的方案评估
报告

方案编制方、委托单位确
认的无误的报告内容

4.安全性
审查

审核报告

委托单位确认的方案评估
报告、密码应用方案

报告审核意见、审核通过
的方案评估报告

方案或报告中存在的问题、
审核结论、审核签字

5.报告编
制

输出报告

审核通过的方案评估报告

正式的方案评估报告

最终确认无误的报告内容

6.方案变
更评估

密码应用方案进行关键性更改需要进行变更评估

1. 总体要求

需要变更评估的条件



密码应用方案评估完成后，委托单位对密码应用方案进行了关键性的更改

2. 评估准备

工作内容

当前阶段的方案评估方应根据方案变更情况出具评估意见，并根据评估意见确定是否重新开展方案整体评估工作

主要任务

确定变更内容

- a) 委托单位出具《密码应用方案变更评估文件》（见附录D），注明更改内容等，并签字、盖章确认。
- b) 评估人员了解系统变更情况，并对系统变更内容、原因、影响范围进行确认

出具评估意见

- a) 根据《密码应用方案变更评估文件》确定变更类型（重大变更或一般变更）；
- b) 一般变更：仅对变更内容结合方案进行评估，并结束当前活动；
- c) 重大变更：需要对更改后的密码应用方案重新开展整体评估

3. 评估修正

4. 安全性审查

附：方案变更评估输入输出物表

任务	输入文档	输出文档	输出文档内容
确定变更内容	密码应用方案	《密码应用方案变更评估文件》	密码应用方案变更原因、变更内容、原方案对比、系统责任人签字、系统责任人所在组织印章
出具评估意见	《密码应用方案变更评估文件》、变更后的密码应用方案	出具评估意见的《密码应用方案变更评估文件》	评估人员的评估意见、评估时间、评估人员签字

5. 报告编制

6. 方案变更评估

附录D-密码应用方案变更评估文件

1.总体要求

2.评估准备

3.评估修正

4.安全性审查

5.报告编制

6.方案变更评估

系统名称	方案名称	变更原因	变更内容	评估意见
系统名称内容	方案名称内容	变更原因内容	- 变更内容 <u>委托单位签字盖章</u> - 日期	<u>变更类型选择</u>：重大变更、一般变更 - 评估意见内容 <u>评估人员签字</u> <u>方案评估方签字</u> - 日期

更新解读

01 密评背景介绍

02 密评管理办法

03 密评总体要求

04 密评测评过程

05 密评团标解读

06 密评FAQ解读

07 密改方案实践



《商用密码应用安全性评估FAQ》（第三版）更新发布

根据相关工作安排，中国密码学会密评联委会组织修订的《商用密码应用安全性评估FAQ》（第三版）已于2023年10月发布，该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，用于替代2022年8月发布的《商用密码应用安全性评估FAQ》（第二版），以帮助相关人员更好开展商用密码应用与安全性评估工作。



《商用密码应用安全性评估FAQ》

2021年12月

《商用密码应用安全性评估FAQ》
(第二版)

2022年8月

《商用密码应用安全性评估FAQ》
(第三版)

2023年10月

文件意义：为密码应用及商用密码应用安全性评估人员的评估工作提供指引

2023年10月，中国密码学会密评联委会发布《商用密码应用安全性评估FAQ》（第三版），用于替代2022年8月发布的《商用密码应用安全性评估FAQ》（第二版），旨在：

- 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
- 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



第一版

全文共解答了22个问题，主要包括信息系统密码应用基本要求的等级、应/宜/可测评指标把握、密钥安全符合性判定、各层测评对象确定、测评对象选取粒度、远程管理通道安全、合规密码产品身份鉴别/完整性相关指标的判定等内容。

第二版

全文共解答了26个问题，目录内新增内容如下：

- 重要数据完整性保护的实现方法问题
- 通过代码实现数据机密性、完整性保护的判定方法
- 网络层安全接入认证和身份鉴别指标的差别
- 应用层身份鉴别是否可以缓解网络层身份鉴别的高风险

第三版

全文共解答了通用类、密码应用技术类、密码应用管理类、量化评估类、风险判定类、特殊场景类等6个部分共56个问题。

第三版修订情况说明

序号	原文	修改情况	备注
1	1.1	新增内容	关于商用密码应用安全性评估的适用范围
2	1.2	新增内容	关于商用密码应用安全性评估的评估对象
3	1.3	新增内容	关于商用密码应用安全性评估的评估方法
4	1.4	新增内容	关于商用密码应用安全性评估的评估结果
5	1.5	新增内容	关于商用密码应用安全性评估的评估流程
6	1.6	新增内容	关于商用密码应用安全性评估的评估工具
7	1.7	新增内容	关于商用密码应用安全性评估的评估人员
8	1.8	新增内容	关于商用密码应用安全性评估的评估环境
9	1.9	新增内容	关于商用密码应用安全性评估的评估记录
10	1.10	新增内容	关于商用密码应用安全性评估的评估报告
11	1.11	新增内容	关于商用密码应用安全性评估的评估总结
12	1.12	新增内容	关于商用密码应用安全性评估的评估改进
13	1.13	新增内容	关于商用密码应用安全性评估的评估反馈
14	1.14	新增内容	关于商用密码应用安全性评估的评估持续改进
15	1.15	新增内容	关于商用密码应用安全性评估的评估持续改进
16	1.16	新增内容	关于商用密码应用安全性评估的评估持续改进
17	1.17	新增内容	关于商用密码应用安全性评估的评估持续改进
18	1.18	新增内容	关于商用密码应用安全性评估的评估持续改进
19	1.19	新增内容	关于商用密码应用安全性评估的评估持续改进
20	1.20	新增内容	关于商用密码应用安全性评估的评估持续改进
21	1.21	新增内容	关于商用密码应用安全性评估的评估持续改进
22	1.22	新增内容	关于商用密码应用安全性评估的评估持续改进
23	1.23	新增内容	关于商用密码应用安全性评估的评估持续改进
24	1.24	新增内容	关于商用密码应用安全性评估的评估持续改进
25	1.25	新增内容	关于商用密码应用安全性评估的评估持续改进
26	1.26	新增内容	关于商用密码应用安全性评估的评估持续改进
27	1.27	新增内容	关于商用密码应用安全性评估的评估持续改进
28	1.28	新增内容	关于商用密码应用安全性评估的评估持续改进
29	1.29	新增内容	关于商用密码应用安全性评估的评估持续改进
30	1.30	新增内容	关于商用密码应用安全性评估的评估持续改进
31	1.31	新增内容	关于商用密码应用安全性评估的评估持续改进
32	1.32	新增内容	关于商用密码应用安全性评估的评估持续改进
33	1.33	新增内容	关于商用密码应用安全性评估的评估持续改进
34	1.34	新增内容	关于商用密码应用安全性评估的评估持续改进
35	1.35	新增内容	关于商用密码应用安全性评估的评估持续改进
36	1.36	新增内容	关于商用密码应用安全性评估的评估持续改进
37	1.37	新增内容	关于商用密码应用安全性评估的评估持续改进
38	1.38	新增内容	关于商用密码应用安全性评估的评估持续改进
39	1.39	新增内容	关于商用密码应用安全性评估的评估持续改进
40	1.40	新增内容	关于商用密码应用安全性评估的评估持续改进
41	1.41	新增内容	关于商用密码应用安全性评估的评估持续改进
42	1.42	新增内容	关于商用密码应用安全性评估的评估持续改进
43	1.43	新增内容	关于商用密码应用安全性评估的评估持续改进
44	1.44	新增内容	关于商用密码应用安全性评估的评估持续改进
45	1.45	新增内容	关于商用密码应用安全性评估的评估持续改进
46	1.46	新增内容	关于商用密码应用安全性评估的评估持续改进
47	1.47	新增内容	关于商用密码应用安全性评估的评估持续改进
48	1.48	新增内容	关于商用密码应用安全性评估的评估持续改进
49	1.49	新增内容	关于商用密码应用安全性评估的评估持续改进
50	1.50	新增内容	关于商用密码应用安全性评估的评估持续改进
51	1.51	新增内容	关于商用密码应用安全性评估的评估持续改进
52	1.52	新增内容	关于商用密码应用安全性评估的评估持续改进
53	1.53	新增内容	关于商用密码应用安全性评估的评估持续改进
54	1.54	新增内容	关于商用密码应用安全性评估的评估持续改进
55	1.55	新增内容	关于商用密码应用安全性评估的评估持续改进
56	1.56	新增内容	关于商用密码应用安全性评估的评估持续改进

第1问：如何确定被测信息系统密码应用等级？

修订

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

背景说明：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。



表1 定级要素与安全保护等级的关系

受侵害的客体	对客体所侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全			

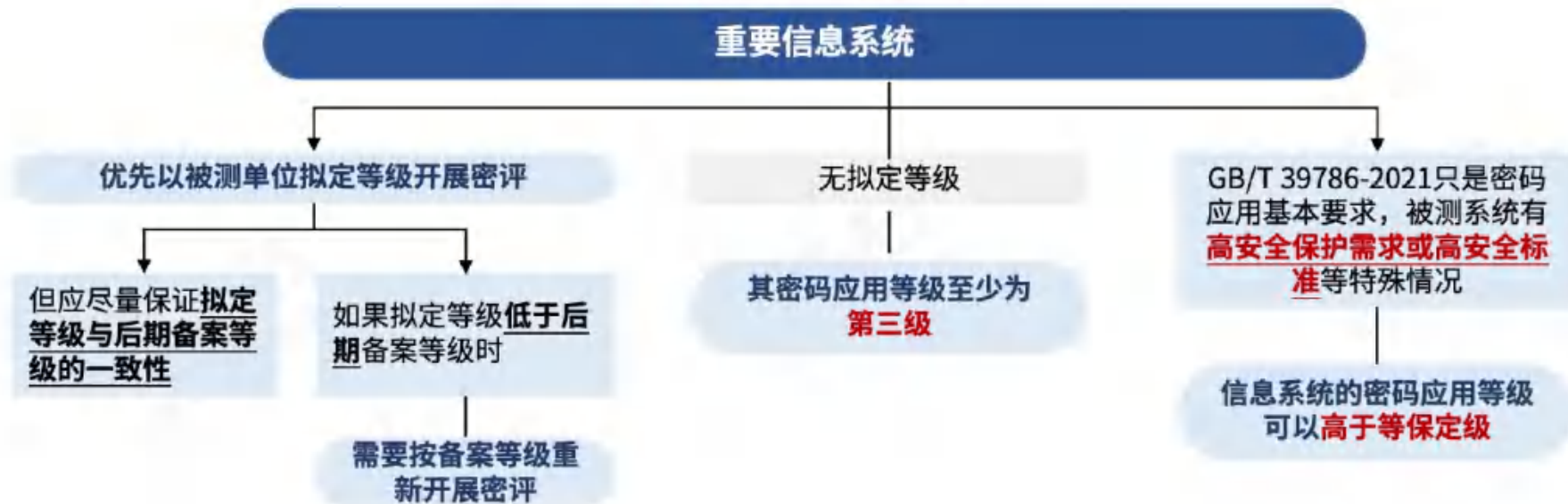
表格来源于：GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

第2问：尚未完成等备案的，如何确定被测信息系统的密码应用等级？

新增 修订

背景说明：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。

未完成网络安全等级保护定级的



第3问：责任单位希望以更高的密码应用要求改造测评信息系统如何把握？

新增

修订

背景说明：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？

等保/密评 级别持平

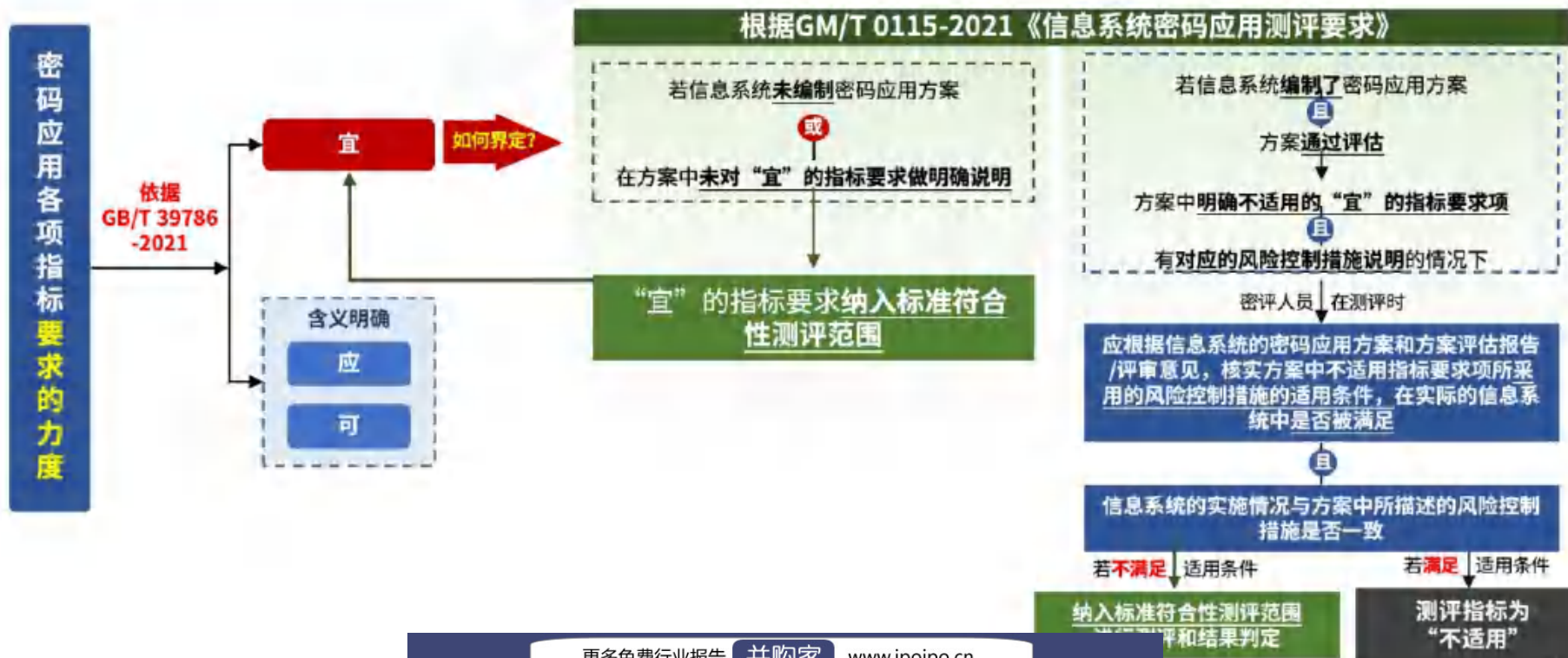
目前，GB/T 39786-2021中的密码应用等级一般与网络安全等级保护的级别持平。所以，在信息系统不存在额外密码应用需求的前提下，原则上被测系统密码应用等级的选取与网络安全等级保护的级别保持一致。

更高等级的密评

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。

第4问：在密评实施中，如何理解和把握“宜”的指标要求？

背景说明：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。



第5问：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？

标准 修订

背景说明：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**。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，评测时如何判定？

对于换证的密码产品

因其换发的认证证书上一律**没有标注**密码模块安全等级
密码厂商提供换**证前的**商用密码产品型号证书

证书中标注了密码模块等级

按此等级进行判定

没有标注等级

按“密码产品符合**一**密码模块”进行判定

对于新发认证证书的密码产品

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

其他产品

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。

第6问：商用密码产品认证证书的有效期限在密评时该如何把握？

新增 修订

背景说明：GM/T 0115《信息系统密码应用测评要求》的通用测评要求中，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；“5.3密码产品合规性”测评要求，在一些特殊情形下的判定要点。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？



认证证书在有效期内：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限内，则可判定为产品合规。

相关标准已失效或更新：在测评过程中，如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。

第7问：如何判断实际部署中涉及客户端的密码产品的合规性？

新增

修订

背景说明：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？

针对此种情况，可分以下三步依次执行测评实施，综合判定产品的合规性。

1

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

- **查看证书确认：**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。
- **厂商提供检测报告确认：**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。

2

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]。

- **服务端/客户端一致性核查：**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。
- **部署与送检产品一致性：**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）。
- **根据密码应用需求等判定合规性：**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

3

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

- **功能一致性：**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。

第8问：如何确定密码产品的密码功能边界，如签名验签服务器实现加解密功能，在测评时如何判定其合规性？

新增

修订



签名验签服务器

这里只针对签名验签服务器实现了加解密功能进行解答。签名验签服务器是在 GM/T 0018-2012《密码设备应用接口规范》的基础上，对服务器密码机进一步封装，以实现签名验签功能。

签名验签服务器在产品检测时，依据以下标准进行检测：

GM/T 0029《签名验签服务器技术规范》

GM/T 0028《密码模块安全技术要求》

除了检测签名验签服务器的签名验签功能外，也检测各算法的加解密功能、性能。

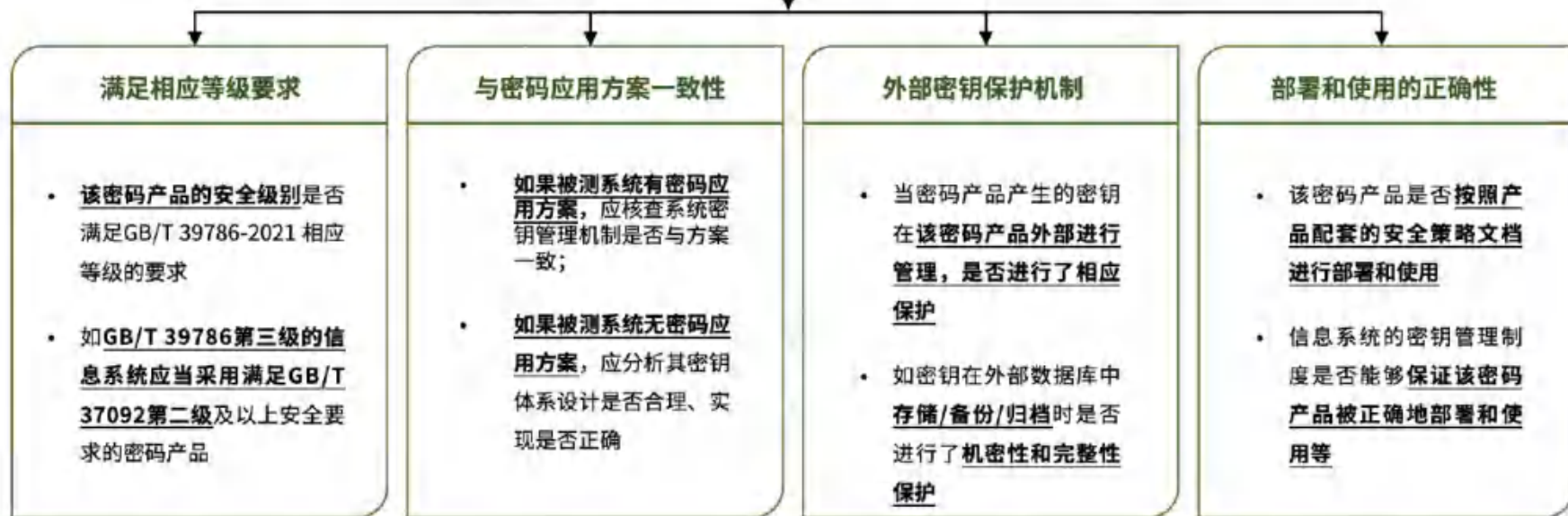
合规
要求

▶ 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。

第9问：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”？

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：



第10问：未使用密码产品，通过开源或自行开发代码软件实现密码算法的方式进行数据机密性、完整性保护，结果怎么判定？是否存在高风险？

新增 修订

《信息安全技术 信息系统密码应用基本要求》GB/T 39786-2021

章	节	指标要求
8 第三级密码应用基本要求	8.4节 应用和数据安全	d) 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机密性
		e) 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。

《信息安全技术 信息系统密码应用基本要求》GB/T 39786-2021

《信息系统密码应用测评要求》GM/T 0115-2021

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

结果判定：不符合

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”。

结果判定：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。

第11问：组合使用密码算法实现数据安全保护时如何量化评估和风险判定？

新增

修订

背景说明：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？

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”）。

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



综合 **DAK** 判定情况进行分析评价

由于算法安全强度和密钥管理、算法实现正确性有关，因此在进行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。

第12问：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？

新增 修订

背景说明：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。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。



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

第13问：针对密码应用方案已经通过评估的信息系统，在密评时发现实际情况不一致，如何处理？

新增

修订

背景说明：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。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

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**

系统运营者

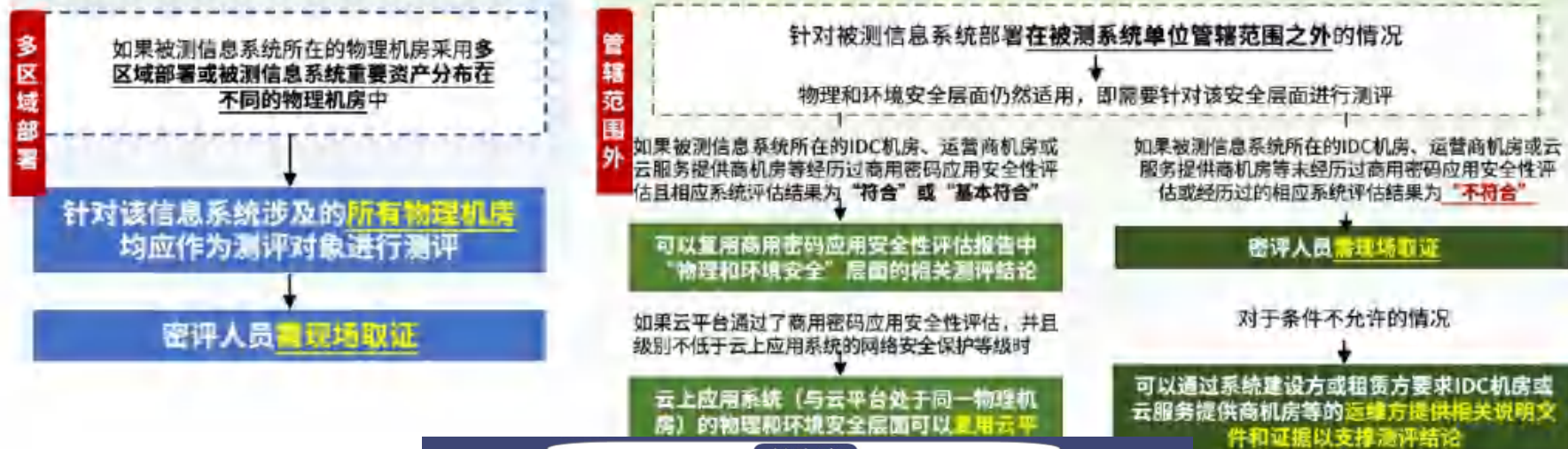
提供密码应用方案修订或优化的证明材料，但同时应按实际测评时掌握的信息为准，并以实际情况得出测评结果。

第14问：如何确定物理和环境安全层的测评对象？对于系统部署在非被测单位管辖范围的情况，在该层应如何判定指标适用性？如何开展密评？

修订

背景说明：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。

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**



第15问：被测信息系统的机房采用多层门禁、且物理访问身份鉴别机制不一致时，物理和环境安全层面的“身份鉴别”指标如何选择测评检查点？

新增

修订

针对此情况需要考虑多层电子门禁系统的保护范围

1

多重保护

如果信息系统所有受保护对象都在多层门禁保护范围内，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。

2

分布在多层门禁中

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，应该以最外层的电子门禁系统作为测评对象。

3

分布在多个门禁中

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。

第15问（续）：被测信息系统的机房采用多层门禁、且物理访问身份鉴别机制不一致时，物理和环境安全层面的“身份鉴别”指标如何选择测评检查点？

新增 修订

接上页



- 可选择一个密码应用最合规、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。

应选择门禁1测评。

门禁1和门禁2都需要测评。

第16问：符合标准的电子门禁系统是否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？

新增 修订

背景说明：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。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？

由于 GM/T 0036 中规定的相关要求，主要针对的是采用**基于非式卡的门禁系统**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：

一是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



二是提供实现该密码应用的密码产品检测认证合规性的证明

网络类型	通信主体
------	------

这里的跨网络访问指的是从不受保护的网路区域访问被阻塞

 用户

测评对象

- ① - ~ - ⑧ -

序号	网络	通信信道	密码应用主要测评
1	政务外网	非国密浏览器与前台应用系统之间的通信信道	HTTPS协议
2		国密浏览器与前台应用系统之间的通信信道	
3		IPSec VPN与IPSec VPN之间的通信信道	
4	政务外网与内网间	政务外网VPN客户端与内网SSL VPN之间的通信信道	SSL VPN协议
5	办公内网	国密浏览器与前台管理系统之间的通信信道	HTTPS协议
6		非国密浏览器与前台应用系统之间的通信信道	
7	互联网	国密浏览器与前台应用系统之间的通信信道	
8		VPN客户端与国密SSL VPN之间的通信信道	



第18、19问：通信信道和内网系统测评

被测系统与第三方电子认证服务相关系统间的通信信道测评

Q 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？

A 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。

不能跨网远程运维的内网系统测评

Q 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？

A

- 这类情况下还需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选择，不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，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。

第20问：双活机房间的通信链路，是否可作为网络和通信层面的通信信道？

新增 修订

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GM/T 0115《信息系统密码应用测评要求》进行测评。

对于双活机房之间的通信链路是物理传输的裸光纤的情况，若**不将**该通信信道作为网络和通信安全层面的测评对象

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**自行评估或密评机构审定**后按实际情况处理

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

节点受控情况

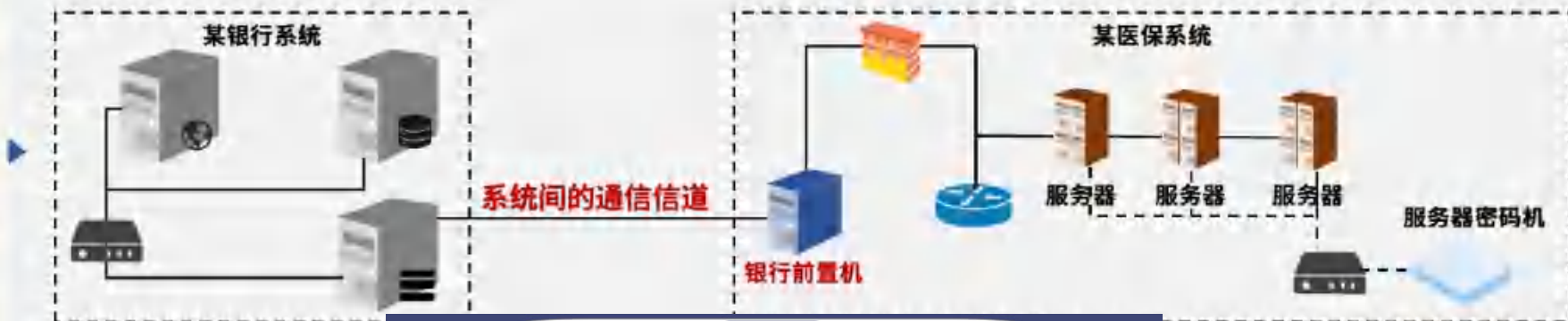
第21问：跨网络边界系统之间的交互，如果通信主体不在其责任范围之内，此通信信道是否需要纳入测评范围？

新增

背景说明：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归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。

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。如下图所示，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”。

存在系统间通信信道的场景



第22问：采用合规的SSL VPN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？

新增 修订

背景说明：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。

单向身份鉴别

针对网络和通信安全层面的“单向身份鉴别”，由于考虑到客户端**不需要对私钥进行密钥管理**（无私钥参与密码运算的需求），因此量化评估中D、A、K最高可为D（√）、A（×）、K（√）。

双向身份鉴别

针对网络和通信安全层面的“双向身份鉴别”，由于在客户端**需要进行密钥运算**，如果采用的是通用浏览器，密钥管理上存在安全问题，因此D、A、K最高可为D（√）、A（×）、K（×）。

第23问：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，确保接入设备身份真实性”，安全接入认证和身份鉴别如何区分？

修订

“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：



“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：



第24问：如何确定设备和计算安全层面的测评对象？

	《信息系统密码应用测评要求》 GM/T 0115-2021	商用密码应用安全性评估FAQ（第三版）
设备和计算层面的测评对象	通用设备（及其操作系统、数据库管理系统）	例如：通用服务器（如应用服务器、数据库服务器）等 例如：数据库管理系统等
	网络及安全设备	
	密码设备	例如：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
	各类虚拟设备	
	提供相应密码功能的密码产品	例如：整机类和系统类的密码产品等
	-	<u>若存在管理通道跨越边界的情况</u> ，需在网络和通信安全层面梳理一条 <u>远程管理数据传输通道</u> 作为测评对象
不属于	-	<u>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</u> 设备和计算安全层面的测评对象
建议	-	在密评报告中，对设备和计算层面的测评对象进行 <u>分类整理和描述</u> 。 <u>至少分为以下6类：</u>
	-	1.密码产品/设备 2.具有密码功能的网络及安全设备 3.采用密码技术的其他产品 4.通用设备 5.不具有密码功能的网络及安全设备 6.虚拟设备和系统

第25问：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？

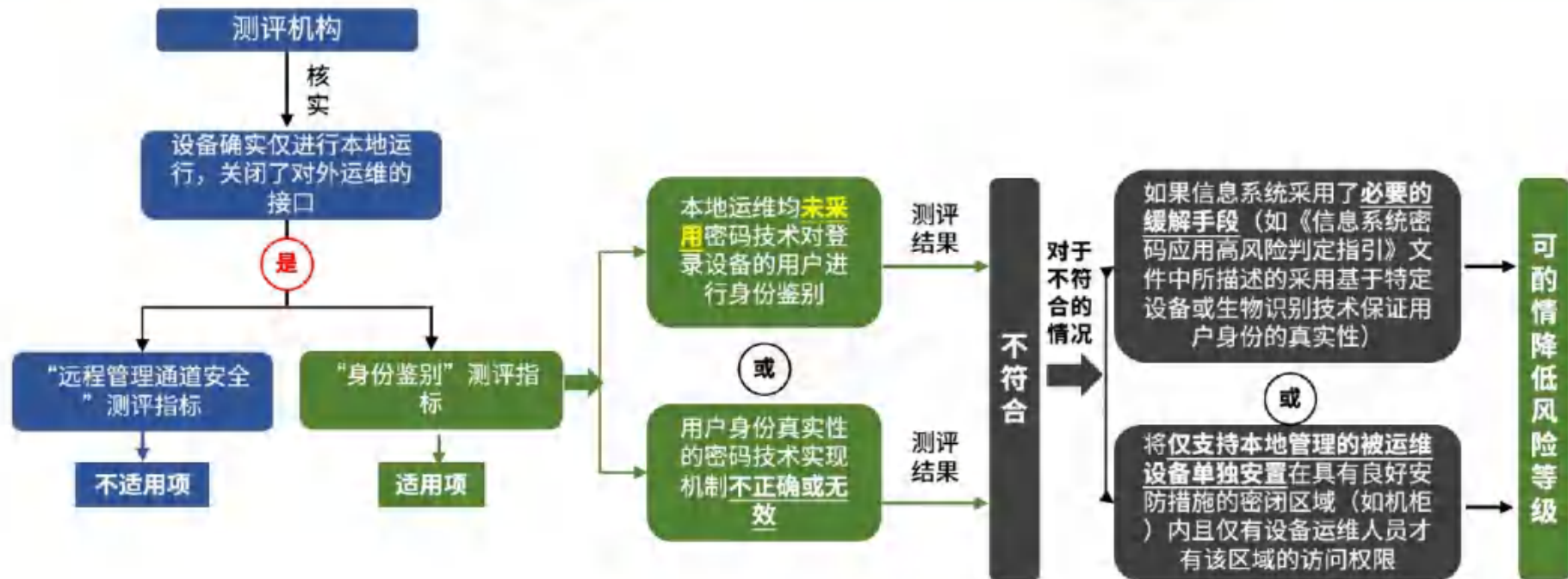
背景说明：设备和计算安全层面的测评对象为通用服务器（如应用服务器、数据库服务器）、数据库管理系统、整机类和系统类密码产品、堡垒机等。在一些较大型信息系统中，针对上述每一类测评对象，普遍都会部署多台设备（如部署多台服务器或者部署服务器集群，部署多台IPSec VPN以与不同的外界通信实体建立通信信道）。在这种情况下，在编写《商用密码应用安全性评估报告》时，设备和计算安全层面各个测评对象确定结果所选取的粒度会影响报告最后得分。

测评对象		通用服务器和堡垒机	整机类密码产品 (如IPSec VPN网关、SSL VPN网关、安全认证网关、数据库密码机、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)
测评对象选取的粒度		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“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	
案例	背景	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	以商用密码产品为例： 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	
	测评对象确定结果	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	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	
	量化评估	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。	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	

* 注：D/A/K源自密评委员会《商用密码应用安全性评估量化评估规则》中的“量化指标”，其中D是密码使用有效性(Cryptography Deployment effectiveness)，A是密码算法/技术合规性(Cryptography Algorithm/Technique compliance)

第26问：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”进行测评和结果判定？

背景说明：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。



第27问:设备和计算安全层面,堡垒机及所运维设备身份鉴别合规性如何判定?

新增 修订

背景说明: 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合规性如何判定?



第28问：设备和计算安全层面，什么情况下堡垒机及被运维设备身份鉴别可酌情降低风险等级？

修订

风险判定

遇有以下情况可以酌情降低风险等级



直接通过堡垒机运维

如果堡垒机的身份鉴别指标的测评结论为“符合”或“部分符合”，且没有高风险

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



通过 VPN 保护运维通信信道，同时满足以下条件

堡垒机及其被运维的设备身份鉴别可视为采取了风险缓解措施

专用安全网关

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）；

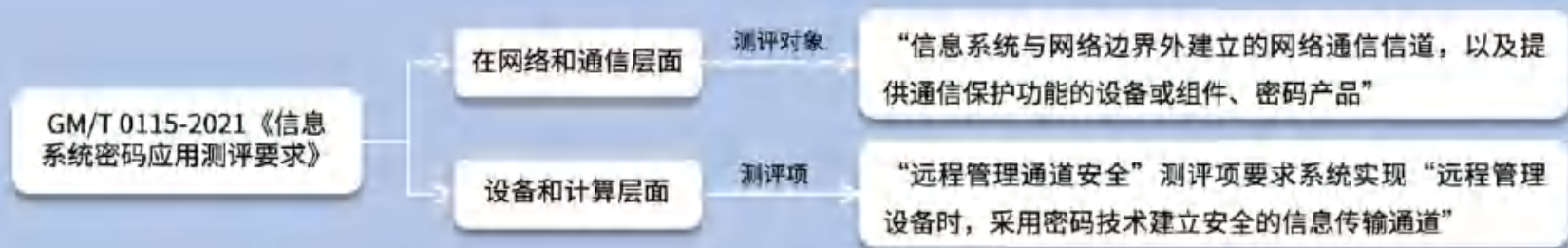
采用密码技术进行通信实体双向身份鉴别

- 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，并且在对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。

第29问：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测评对象重复测评，如何进行量化评估？



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。



第29问（续）：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测评对象重复测评，如何进行量化评估？



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

第30问：合规密码产品设备和计算安全层面的指标，应该如何测评？

修订

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

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



合规密码产品的

- 1 “身份鉴别”
- 2 “系统资源访问控制信息完整性”
- 3 “日志记录完整性”
- 4 “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？

整机类密码产品

系统类密码产品

其软件部分所在服务器和所含整机类密码产品应分别作为设备和计算安全层面的测评对象，并单独实施测评。

具有合格的商用密码产品认证证书

且 实际部署的密码产品与获认证产品一致

安全等级二级及以上的密码产品

安全等级一级的密码产品

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

由于并未要求其软件/固件完整性校验采用带密钥的核准密码技术实现，如确认未采用

进一步判定

保证用户身份真实性

实地查看密码产品是否采用了密码技术：

- 智能IC卡
- 智能密码钥匙
- 动态口令
- ……

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

- 2 “系统资源访问控制信息完整性”
- 3 “日志记录完整性”
- 4 “重要可执行程序完整性、重要可执行程序来源真实性”等

1 “身份鉴别”

不能直接判定为符合

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

判定为“符合”

判定“身份鉴别”指标的“密钥管理安全性”为“不符合”

第31问：如何确定应用和数据安全层面的测评对象？

《信息系统密码应用测评要求》
GM/T 0115-2021



在应用和数据层面的测评对象为
“业务应用以及重要数据”

应用和数据安全层面测评对象确定：

测评对象应包含
关键业务应用

有密码应用方案

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

无密码应用方案

根据网络安全等级保护定级报告描述
的范围确定

一般情况下应包含被测系统的所有业务应用

鉴别数据

重要业务数据

重要审计数据

个人敏感信息

法律法规规定的其他重要数据类型

.....

第32问：在云应用/平台测评中，密码资源池的密码管理平台是哪个层面的测评对象？



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？



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的一个管理类应用系统**进行测评。

第33问：某些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？

新增

修订

信息系统所在行业
关于数据分级的标准和要求

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）

结合

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。

第34问：信息系统使用了第三方提供的数据异地备份的服务，如备份在第三方提供的异地机房中，备份数据是否纳入测评范围？

新增

修订

备份数据密码应用需求与生产数据一致

备份数据作为生产数据的副本，其密码应用需求与生产数据一致。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。

编写密评报告可将备份数据同生产数据合并处理

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结果为“部分符合”。

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。

第35问：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？

新增

修订

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。

已通过密评第三方身份认证服务系统

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。

未通过密评或未做密评的第三方身份认证服务系统

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。

第36问：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？

新增 修订

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**。

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）或数字签名的方式实现数据存储的完整性

本部分定义了 8 种采用 n 比特分组密码的消息鉴别码算法（MAC 算法）：CBC-MAC、EMAC、ANSI retail MAC、MacDES、CMAC、LMAC、TrCBC、CBCR。

本部分定义的第一个 MAC 算法通常被称作 CBC-MAC。其余七个 MAC 算法是 CBC-MAC 的变种。其中，MAC 算法 2、MAC 算法 3、MAC 算法 5、MAC 算法 6 和 MAC 算法 8 在操作的末尾应用了特殊的变换。MAC 算法 4 在操作的起始和末尾各应用了一个特殊的变换。MAC 算法 7 在截取 MAC 值时使用特殊的规则。当 MAC 算法的密钥长度是分组密码密钥长度的两倍的时候，宜使用 MAC 算法 4。MAC 算法 5 和 MAC 算法 7 使用加密的次数最少。MAC 算法 5 只需要一次分组密码密钥设置，但需要一个较长的中间密钥。MAC 算法 6 是 MAC 算法 2 的可选变种。MAC 算法 7 和 MAC 算法 8 不需要中间密钥和密钥设置，当存储空间受限时，建议使用 MAC 算法 7 和 MAC 算法 8。

本部分凡涉及密码算法的相关内容，按国家有关法规实施；凡涉及采用密码技术解决保密性、完整性、真实性、抗抵赖性需求的宜遵循密码相关国家标准和行业标准。

图片来源：《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》（GB/T 15852.1-2020）

GB/T 15852.1-2020 中定义了8种采用 n 比特分组密码的消息鉴别码算法（MAC算法）

CBC-MAC	EMAC	ANSI retail MAC	MacDES	CMAC	LMAC	TrCBC	CBCR
---------	------	-----------------	--------	------	------	-------	------

第37问：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？

新增

修订

分组密码的 ECB 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。

不推荐在密码应用中使用 ECB 模式，
并且在测评时应告知对方安全风险

若有明显安全风险，应进一步
敦促其改正以免影响风险判定结果。

测评判定

在测评判定时，按照目前测评
的现行准则，可判定为

符合

第38问：如何编写密评报告中应用和数据安全层面的测评对象和测评结果汇总？

新增 修订

背景

在《商用密码应用安全性评估报告模板（2023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。

参考示例：某信息化办公系统（第三级）

简介：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。

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（如右图）。

表 3-7 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	访谈法 ☒ 实地查看 ☒ 工具测试	

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）							不可否认性
		身份鉴别	访问控制 信息完整性	重要信息资源 安全标识完整性	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	
1	信息化办公系统应用	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
	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

第39问：如何编写密评报告中应用和数据安全层面身份鉴别、重要数据传输和存储保护等细粒度的测评对象？

新增 修订

参考示例：某信息化办公系统（第三级）

简介：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。

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（如右图所示）。

表 4-5 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

示例

身份鉴别情况

表 4-6 应用和数据安全重要数据测评结果汇总

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

示例

重要数据的机密性和完整性保护情况

表 4-7 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

示例

不可否认性情况

第40问：如何编写密评报告中应用和数据安全测评结果记录？

新增 修订

- ① 身份鉴别
- ② 访问控制信息完整性
- ③ 重要信息资源安全标记完整性
- ④ 重要数据传输机密性、完整性
- ⑤ 重要数据存储机密性、完整性
- ⑥ 不可否认性

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			测评对象评分 $S_{i,j,k}$	测评单元得分 $S_{i,j} = \frac{\sum_{k=1}^n w_k S_{i,j,k}}{w_j}$
			密码使用安全 D	密码算法/技术合规性 A	密钥管理安全 K		

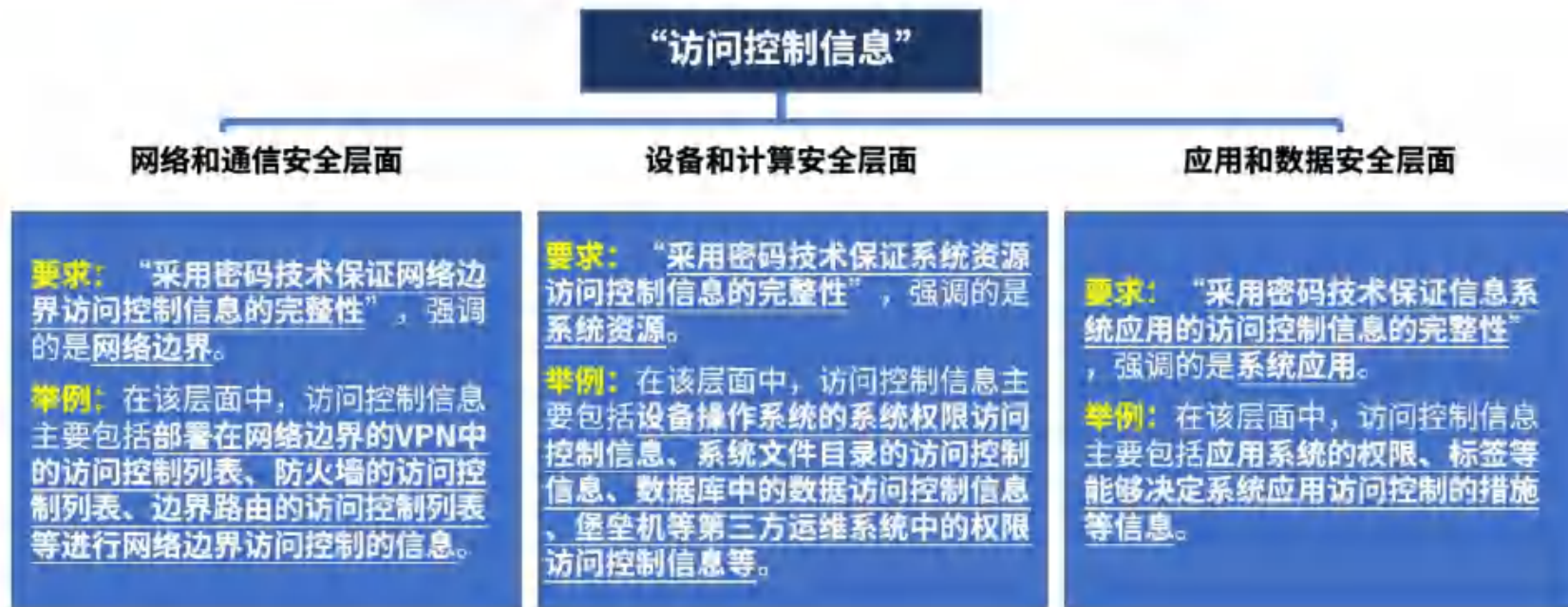
通过 $\sqrt$ 未通过 $\times$

示例

OA 办公系统管理员用户、OA 办公系统业务用户、公文管理系统管理员用户、公文管理系统业务用户、OA 办公系统、公文管理系统、公文管理系统、OA 办公系统管理员用户登录口令、OA 办公系统业务用户登录口令、OA 办公系统业务报表、OA 办公系统办公文件数据、OA 办公系统业务日志、公文管理系统管理员用户登录口令、公文管理系统业务用户登录口令、公文管理系统业务数据、公文管理系统业务日志

第41问：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？

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括但不限于以下方式：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。



第42问：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？

新增 修订

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

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。

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该区域内的所有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。

被测信息系统跨网络边界调用密码资源测评

GM/T 0115-2021《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。

密码资源调用的技术指标测评

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。

第43问：在依据GB/T 39786-2021 9.7 a)条款密评时测评时的密码应用方案该如何理解？

背景

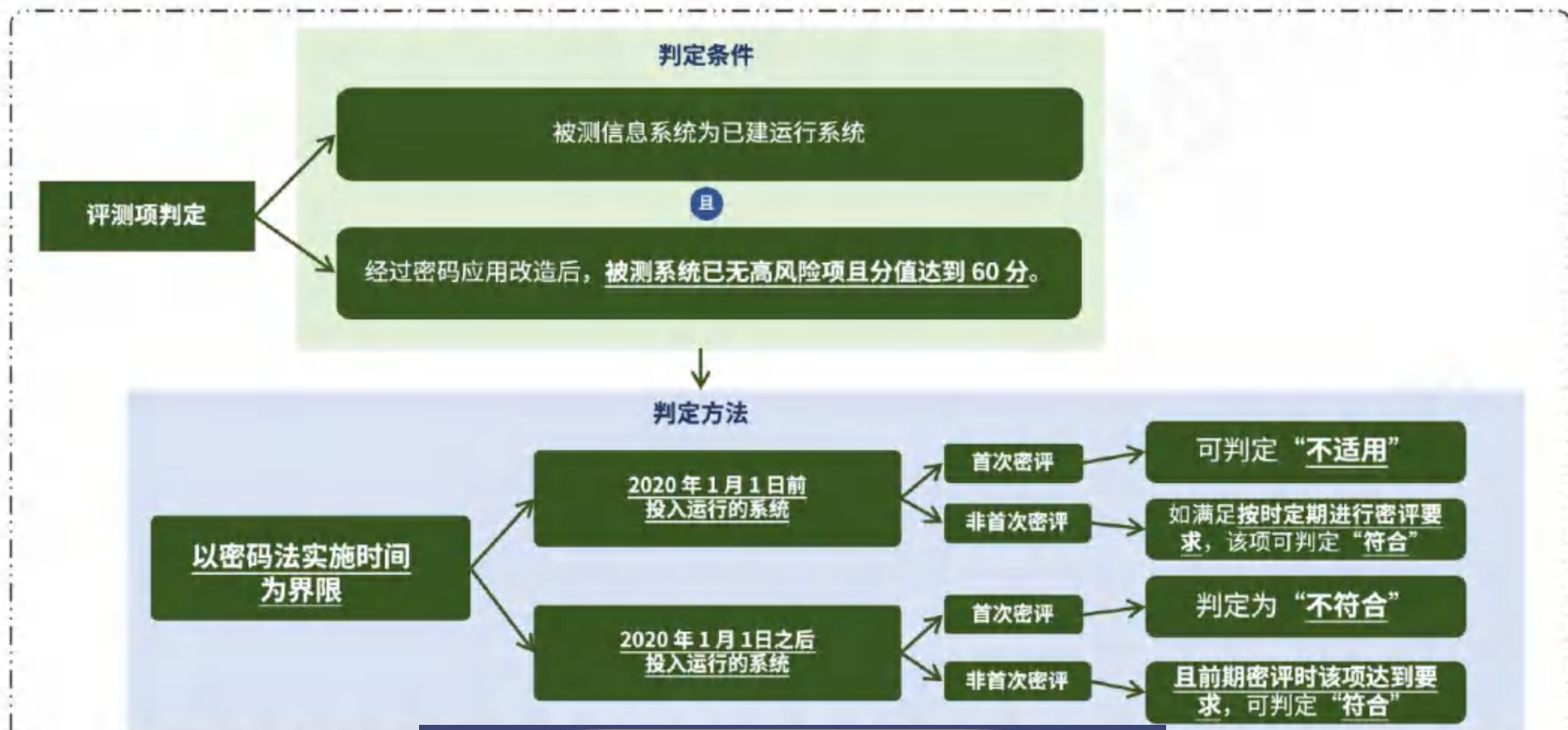
参考标准：GB/T 39786-2021 《信息安全技术信息系统密码应用基本要求》

相关内容：标准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。

关于已建信息系统中密码应用方案的问题以及后续判定依据



第44问：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？



第45问：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？

新增

修订

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。

针对上述信息系统密码应用成熟度很低情况，在密评时仍需将GM/T 0115-2021 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。

管理制度

人员管理

建设运行

应急处置

测评过程中需进一步考察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

被测单位建立了上岗人员培训制度，并规定对涉及密码的操作和管理的人员培训内容，但实际未设置密码的操作和管理的人员岗位或人员上岗时未经过相关培训，

此时**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。

第46问：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？

新增

密码

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)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机密性；e)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。

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；

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。

第47问：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？

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。

风险等级、测评结论、分数是否发生变化？

风险等级	测评结论	分数
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， <u>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。</u>	<u>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</u>	<u>测评分数保持不变</u>

- 本着重点保护重要系统的原则，《信息系统密码应用高风险判定指引》将大部分高风险项调整为适用于第三级以上的系统。
- 网络安全等级保护第三级以下系统，在进行密评时，并非不涉及高风险。密评机构在进行密评时，应参照《信息系统密码应用高风险判定指引》，根据应用系统的实际场景、面临的威胁、存在的安全问题以及缓解措施进行综合风险判定。网络安全等级保护第三级以下系统可参考高风险判定指引执行。
- 根据《信息系统密码应用高风险判定指引》第5章节，通用要求中的密码算法、密码技术、密码产品和密码服务均适用于所有级别信息系统。

第48问：针对测评报告模板中高风险修正过程在哪个地方体现？

新增 修订

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（2023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。	管理和环境	可能导致非法人员进入物理环境，对物理设备和数据进行破坏；但发现外联设备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

第49问：“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？

新增 修订

“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”）。

结合其他层面“身份鉴别”指标测评结果综合考虑

比如，“网络和通信安全”进行对接入的用户设备进行了身份鉴别，但“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”，但需要结合“网络和通信安全”层面的身份鉴别机制和“应用和数据安全”层面相关的工作机制，给出合适的风险等级。

第50问：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）》文件中，部分高风险项安全问题所提到“适用时”该如何理解？

新增

修订

背景

在《信息系统密码应用高风险判定指引（2021）》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”。

《信息系统密码应用高风险判定指引（2021）》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是否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）且该密码产品能否满足应用场景实际需求

存在且能满足

反之

“适用”

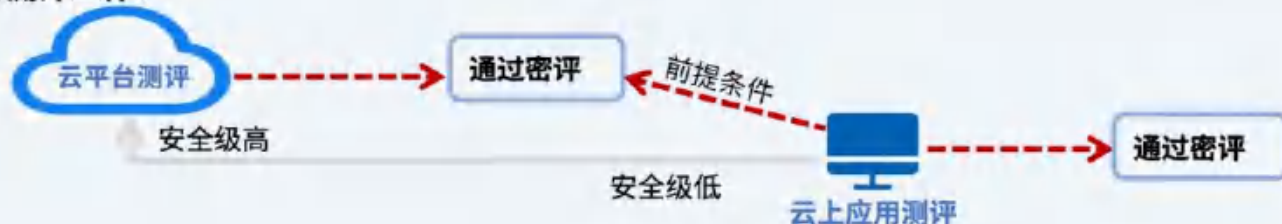
“不适用”

须在密评报告的风险分析环节详细论述原因。

第51问：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？



云平台 and 云上应用两部分测评工作：



第52问：云上应用的部分测评结论需要依赖于云平台的测评结果，对运行在云平台上的云上应用进行密评时，云平台如何测评？

修订

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：

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）。

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）。

第53问：对运行在云平台上的云上应用进行密评时，云上应用如何测评？云平台 and 云上应用的测评结论能够复用吗？

修订

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：

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）。

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。

云上应用系统调用非云平台提供支撑能力

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，或未取得“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

第53问（续）：对运行在云平台上的云上应用进行密评时，云上应用如何测评？云平台和云上应用的测评结论能够复用吗？

新增 修订

表 34-1 被完全评估的支撑能力说明示例

序号	安全属性	被完全评估的密码支撑能力		测评结果		
		测评对象	可能涉及的措施	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	低
2			电子门禁记录数据存储在本地	0.5	部分符合	低
3			视频监控记录数据存储在本地	0.5	部分符合	低
4	网络和通信安全	云平台网络	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	低
6			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	低
7	应用和数据安全	支撑能力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	低

云平台支撑能力说明模版

表 34-2 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	*****
	服务器	√	*****	√	*****	中、低	*****
		×	*****	×	*****	高	*****

第54问：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？

新增



在《商用密码应用安全性评估报告模板（2023版）》“被测信息系统基本信息表”中增加“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单独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。

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。



对于该情况，云平台和密码服务平台（特指已单独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。

第55问：面向公众、信息可公开的信息系统，需要重点关注哪些内容？

首先确定哪些人员可以访问该信息系统：

管理员

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。

公众用户

对网站身份鉴别，内容完整性保护

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

总结：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。

第56问：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？

新增

修订

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。

针对这类定级系统

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。

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

可按照 GB/T 39786-2021、GM/T 0115-2021 的相关要求选取适用指标进行测评。

测评对象选取

应用和数据安全层面

可分析是否存在网络管理等相关的业务，若存在可考虑作为应用和数据安全层面的测评对象。

设备和计算安全层面

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

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。

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

建议

密评机构进一步参考密码应用（或改造）方案、网络安全等级保护测评报告，以确认相关系统开展密评的可行性

01 密评背景介绍

02 密评管理办法

03 密评总体要求

04 密评测评过程

05 密评团标解读

06 密评FAQ解读

07 密改方案实践



公司定位：炼石就是数据安全

炼石是以“免改造”为创新特色的数据安全产品厂商，自研灵活挂载多重安全能力的免改造平台，帮政企客户打造领先数据安全保护体系，同时敏捷交付国密合规改造。



公司布局：产品服务联动，贴身保障客户

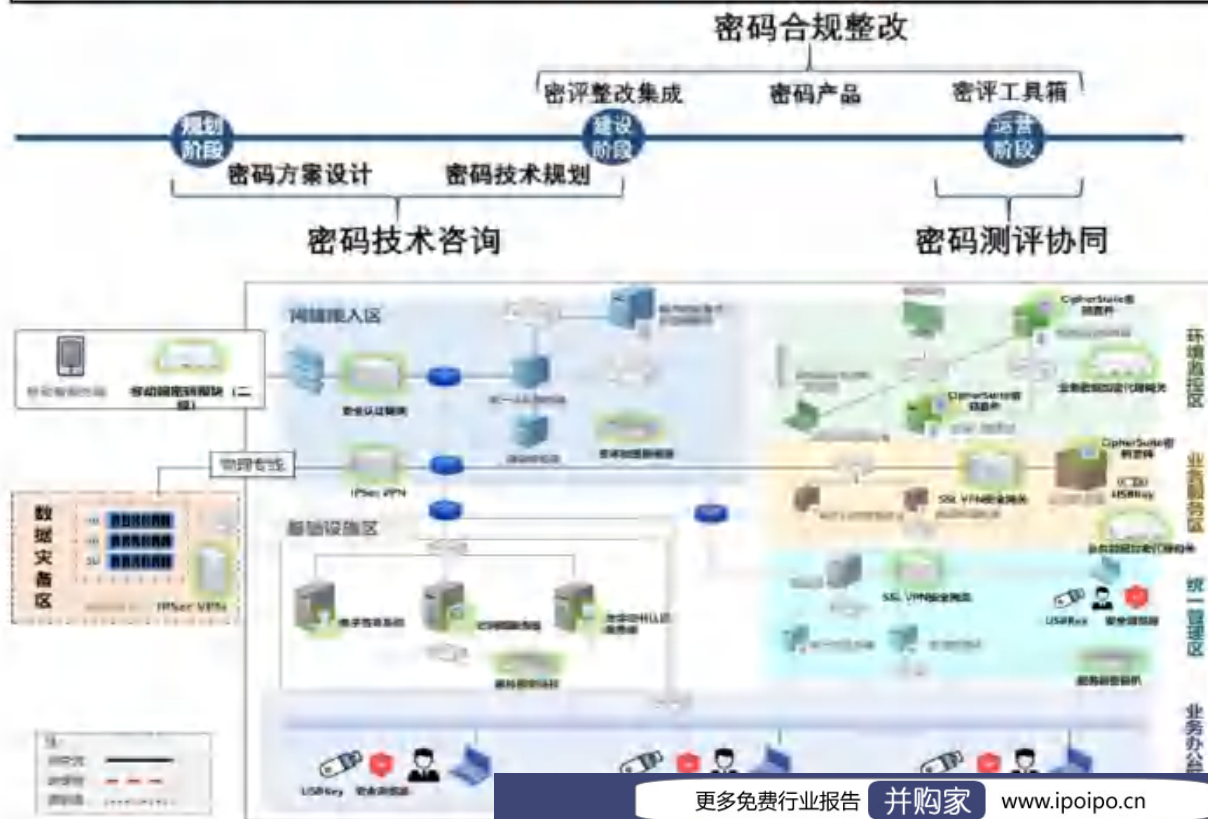
总部位于北京海淀，在重庆、天津、上海等设有子公司，在深圳、西安、成都、沈阳等设有办事处



国密合规场景

一站式密改套餐敏捷交付

炼石国密合规改造方案适用于政务、金融、交通、运营商、医疗、能源、水利、工业等多行业客户开展商用密码应用安全性评估工作，**支持关基、等保三级、政务等重要网络与信息系统**“三同步、一评估”。



① 密码方案咨询

交付形态：技术支持服务

- 结合客户侧业务使命、网络架构、应用模式和编程语言等，考虑从物理和环境、网络和通讯、设备和计算以用应用和数据进行密码方案设计。
- 结合客户侧组织结构、安全体系、人员梯队等，考虑从密码基础知识，密码技术实现，密码工程应用等，提供密码技术体系整体规划。

② 密码合规整改

交付形态：集成服务方案；密码产品；密评工具箱

- 结合GB/T 0054和GB/T 39786中实现要求，为客户侧提供完整的密评方案，确保客户侧密评和等保工作同步；
- 可为客户提供高性能加密组件，结构化数据AOE模块，非结构化数据TFE模块；
- 可为用户提供符合GB/T 0028 GM/T 0005等标准要求的密评工具箱。

③ 密码测评协同

交付形态：技术支持服务

结合客户侧已部署密码设施情况和密码应用情况，协助客户建立全生命周期密钥管理，以及配套的密码管理制度、人员培训、技能提升等。

密码合规的意义：只有正确的使用密码，才能更有效的保障数据安全

密码测评规则

依据	GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
通过要求	60分以上，无高风险
测评规则	打分制，满分100，共41项检测项，包含8个方面
典型问题	无合规的密码设备，无管理制度
评估周期	等保三级系统，每年至少一次

高危风险，一票否决

- 实体间未通过密码技术进行身份鉴别
- 未采用密码技术保证通信过程中重要数据的机密性
- 未采用密码技术对从外部连接到内部的设备进行认证（第四级）
- 未采用密码技术建立安全的信息传输通道，如SSLVPN
- 未采用密码技术保证重要数据在存储过程中的机密性
- 未采用密码技术保证重要数据的完整性
- 未采用密码技术提供数据原发证据和数据接收证据（如有）
- 未建立密码相关管理制度
- 未制定密码应用解决方案、实施方案和应急处置方案，未通过评审

密码合规要点（以等保三级系统为例）

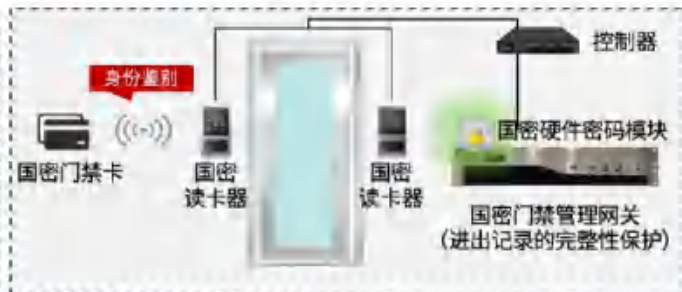
物理和环境	身份鉴别、门禁记录、监控记录、 密码服务资质、密码产品认证	10分
网络和通信	身份鉴别、数据的完整性和机密性、访问控制信息完整性、设备认证、 密码服务资质、密码产品认证	20分
设备和计算	身份鉴别、加密通道、访问控制和安全标记的完整性、日志和程序完整性、真实性、 密码服务资质、密码产品认证	10分
应用和数据	身份鉴别、传输和存储的机密性、完整性、不可否认性、 密码服务资质、密码产品认证	30分
管理制度	包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度	30分
人员管理	角色、职责、权限、审计机制、培训与考核、保密协议	
建设运行	密码应用方案、实施方案	
应急处置	应急处置方案，及时上报	

物理和环境安全技术方案 (10分)

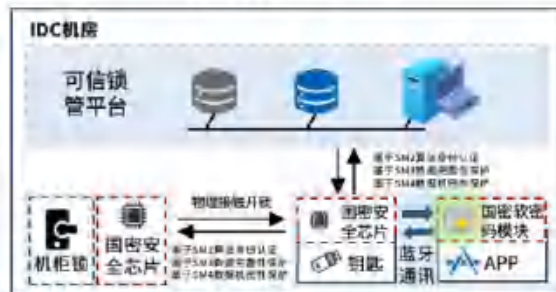
机房视频场景



机房门禁场景



机房机柜锁场景



参数	描述	参数	描述	名称	描述
CPU	2 * ARM Cortex-A55 4核2GHz	存储	4GB+16GB emmc	门禁管理网关	实现门禁管理功能，内置加密卡，实现对门禁进出记录完整性进行保护
操作系统	Linux	通信协议	GB/T 28181、TCP/UDP、SIP	门禁控制器	接收并处理来自应用程序的实时命令
视频输入	16路/32路IPC (最大支持1080P)	视频编码	H.264/H.265	门禁读卡器	键盘读卡器，实现国密身份认证
网络接口	16★10/100/1000Mbps PoE电口 符合IEEE802.3af/at标准	尺寸	480*420*44mm (1U机架式) 720*420*88mm (2U机架式)	门禁卡	CPU卡，实现国密身份认证
环境条件	工作温度: -10°C~55°C 存储温度: -20°C~70°C 湿度: 5%~95%	安全芯片	内置国密国密安全芯片，支持SM1/SM2/SM3/SM4国密算法、AES/DES/RSA/ECC国密算法		
功耗	350W	高可用性	设备内部通过部署双板卡，实现设备高可靠性		

物理和环境安全层面，密评要求指标：

- ①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 (宜)
- ②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 (宜)
- ③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 (宜)

改造方案：

- ①通过国密CPU卡实现人员身份鉴别
- ②通过门禁管理网关上集成安全模块，实现门禁记录完整性保护
- ③通过视频监控一体机对视频数据进行完整性保护

网络和通信安全技术方案 (20分)



网络和通信安全层面，密评要求指标：

- ①应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；（应）
- ②宜采用密码技术保证通信过程中数据的完整性（宜）
- ③应采用密码技术保证通信过程中重要数据的机密性（应）
- ④宜采用密码技术保证网络边界访问控制信息的完整性（宜）
- ⑤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（可）

改造方案：

- ①通过**国密SSL VPN**确保人员身份的真实性
- ②安全网关在通信时通过**SM3-HMAC**运算保障了数据完整性
- ③安全网关创建**国密SSL通道**保障了数据传输的机密性
- ④安全网关通过**SM3-HMAC**对网络边界访问控制信息做完整性运算
- ⑤通过安全网关的**控制策略**对外部接入设备进行权限认证

设备和计算安全技术方案 (10分)



设备和计算安全层面，密评要求指标：

- ①应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（应）
- ②远程管理设备时，应采用密码技术建立安全的信息传输通道（应）
- ③宜采用密码技术保证系统资源访问控制信息的完整性（宜）
- ④宜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（宜）
- ⑤宜采用密码技术保证日志记录的完整性（宜）
- ⑥宜采用密码技术对重要可执行程序进行完整性保护，对其来源进行真实性验证（宜）

改造方案：

- ①通过UKey+数字证书或国密动态口令确保登录堡垒机用户的身份鉴别
- ②远程管理通道安全性借助安全网关能力，构建安全传输通道
- ③通过加密卡签名对堡垒机中的访问控制信息完整性保护
- ④重要信息资源安全标记的完整性（不适用）
- ⑤通过加密卡对日志记录进行签名，保障日志完整性
- ⑥调用加密机对重要可执行程序完整性，来源真实性

应用和数据安全技术方案 (30分)



难度最大
最贴合业务
影响范围最广
属于高风险项

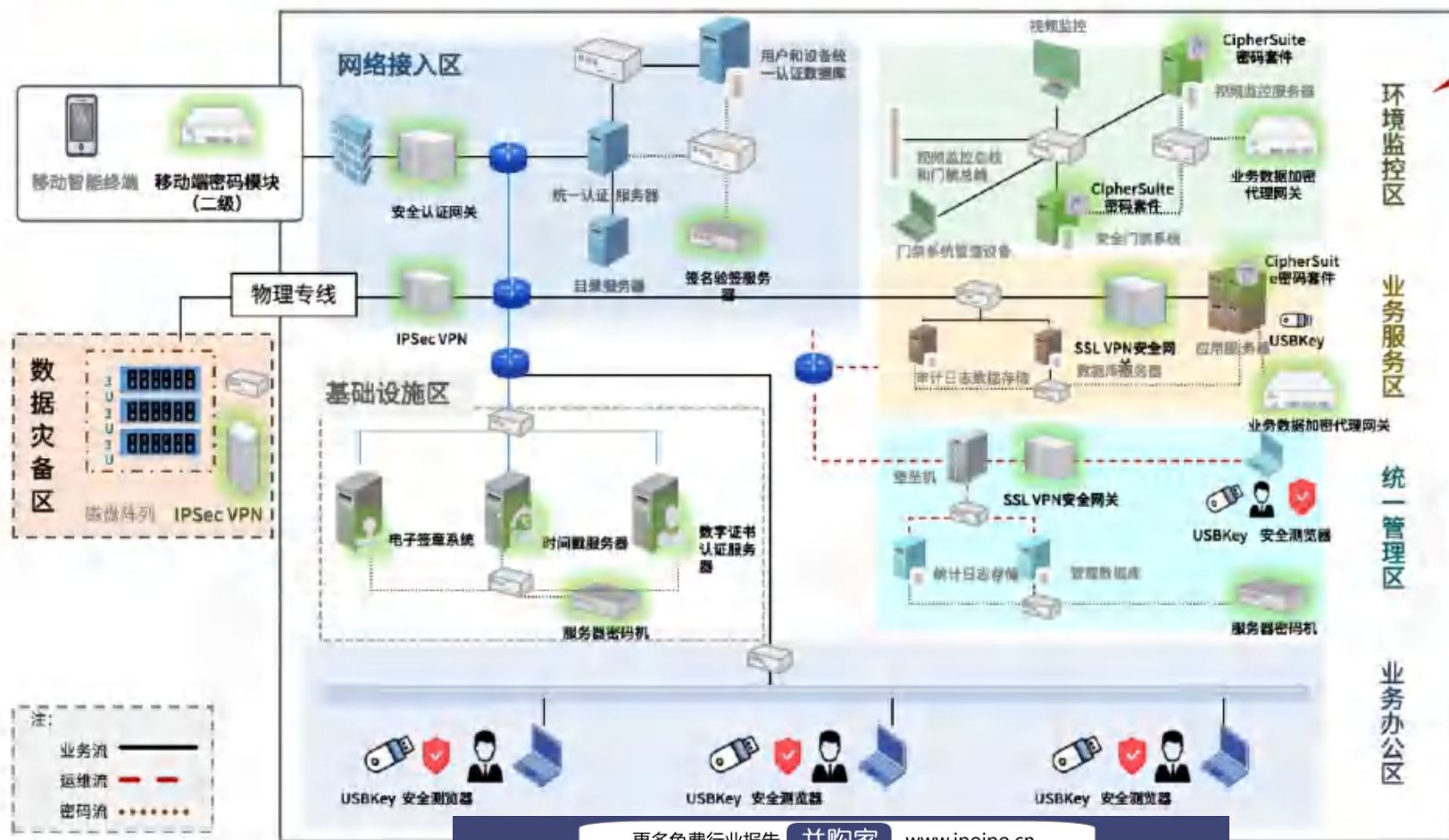
应用和数据安全层面，密评要求指标：

- ①应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（应）
- ②宜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（宜）
- ③宜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（宜）
- ④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（应）
- ⑤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（应）
- ⑥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（宜）
- ⑦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（宜）
- ⑧在可能涉及法律责任认定的应用中，宜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（宜）

改造方案：

- ①通过UKey+数字证书或国密动态口令确保应用用户、管理员、审计员在应用端身份的真实性；
- ②应用程序通过签名验签服务器的签名/HMAC运算，保证访问控制信息完整性；
- ③通过调用签名签名服务器对重要信息资源安全标记的进去签名
- ④⑥外界接入数据机密性、完整性可通过安全网关保证；网内模块之间数据通信适用国密SSL通道做保障；
- ⑤⑦数据存储的机密性、完整性可通过数据库/文件加密实现；
- ⑧通过调用签名/验签技术确保原发证件、接受证据行为的不可否认性。

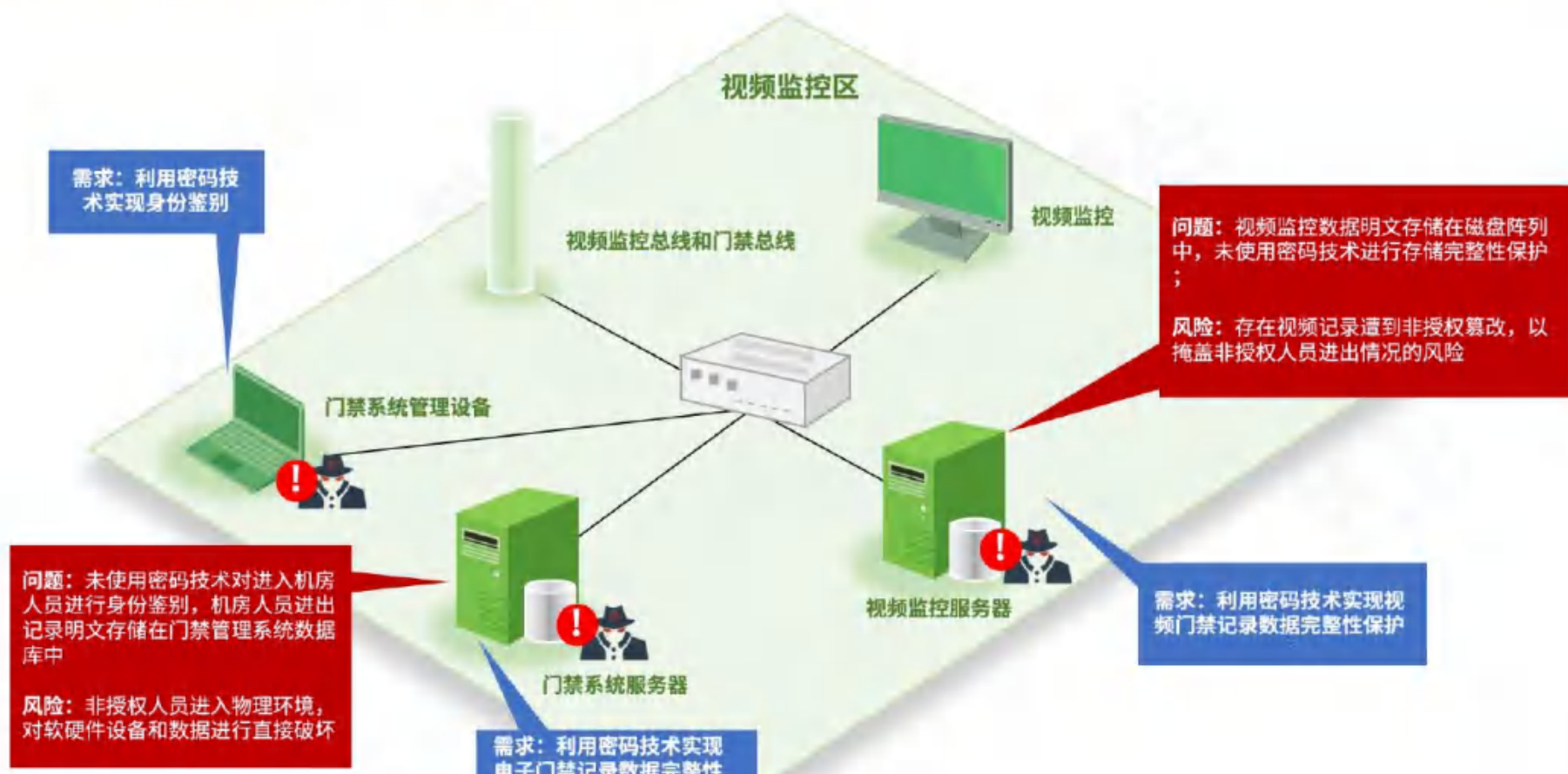
密改方案：以应用为抓手的免改造密评合规示例



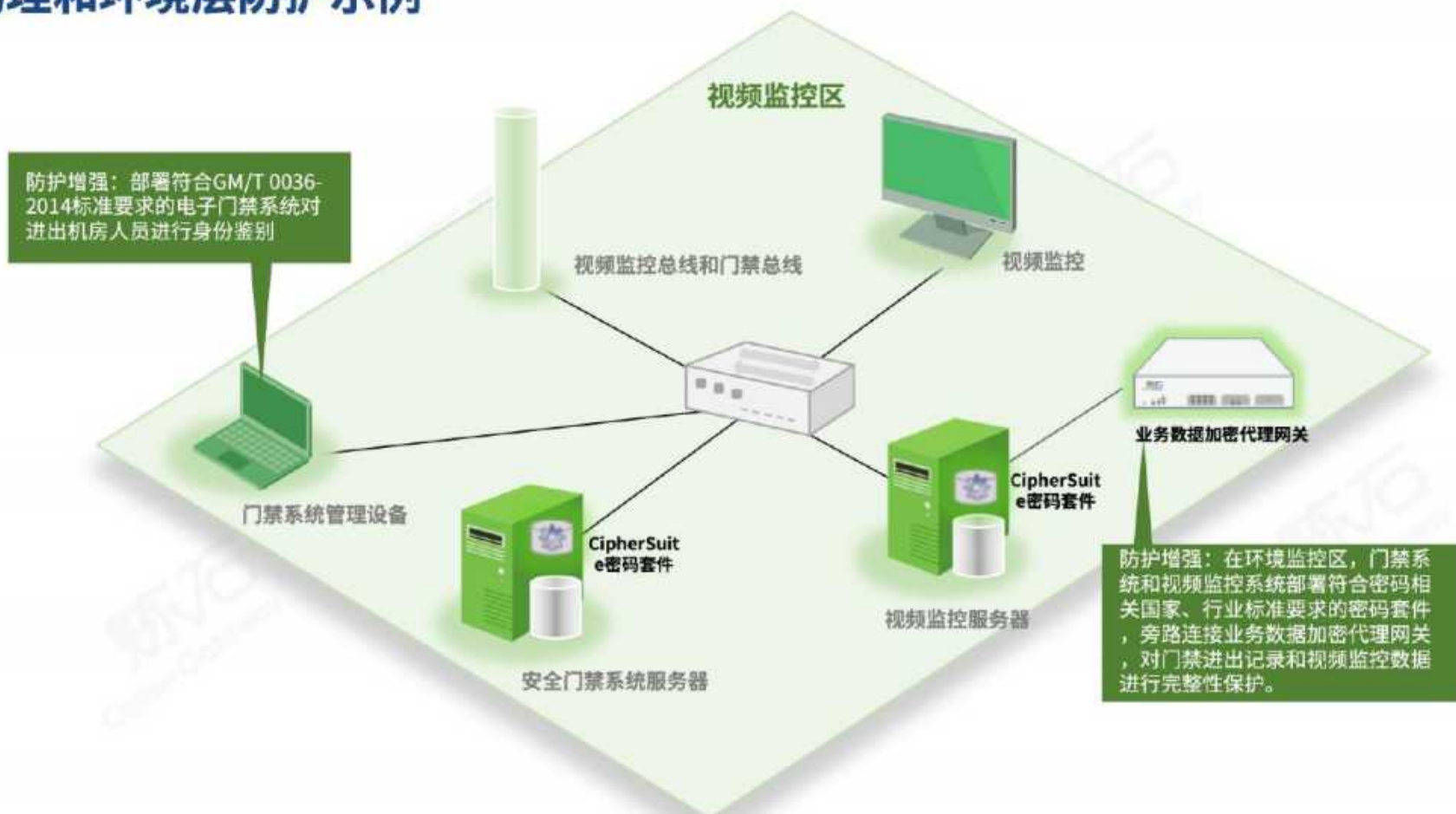
将安全模块内嵌于本地应用中，可以在不改造成应用的情况下，提供面向服务侧的数据存储加密、面向用户侧的动态脱敏及审计，以应用为抓手，打造“以密码技术为核心、多种技术相互融合的新数据安全保护体系”。

(1) 物理和环境安全

物理和环境层风险分析与密码需求



物理和环境层防护示例



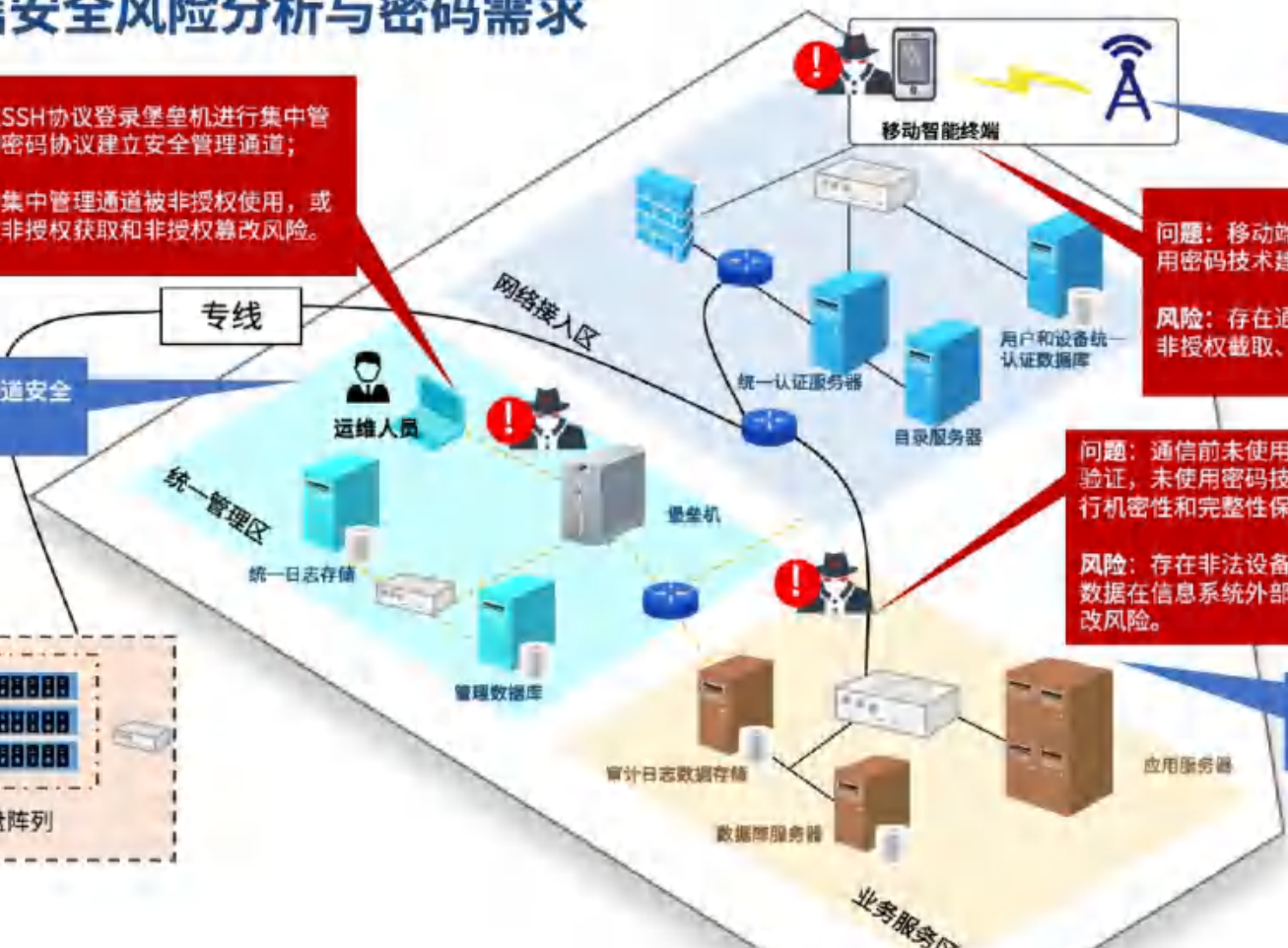
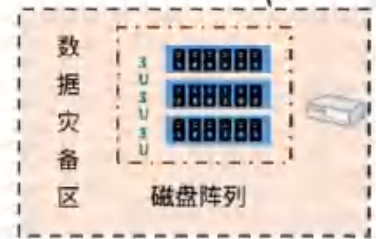
(2) 网络和通信安全

网络和通信安全风险分析与密码需求

问题：管理员通过SSH协议登录堡垒机进行集中管理，未使用合规的密码协议建立安全管理通道；

风险：存在搭建的集中管理通道被非授权使用，或传输的管理数据被非授权获取和非授权篡改风险。

需求：集中管理通道安全密码模块实现



需求：通信数据完整性，通信数据机密性

问题：移动端App使用HTTP协议，未使用密码技术建立安全的数据传输通道；

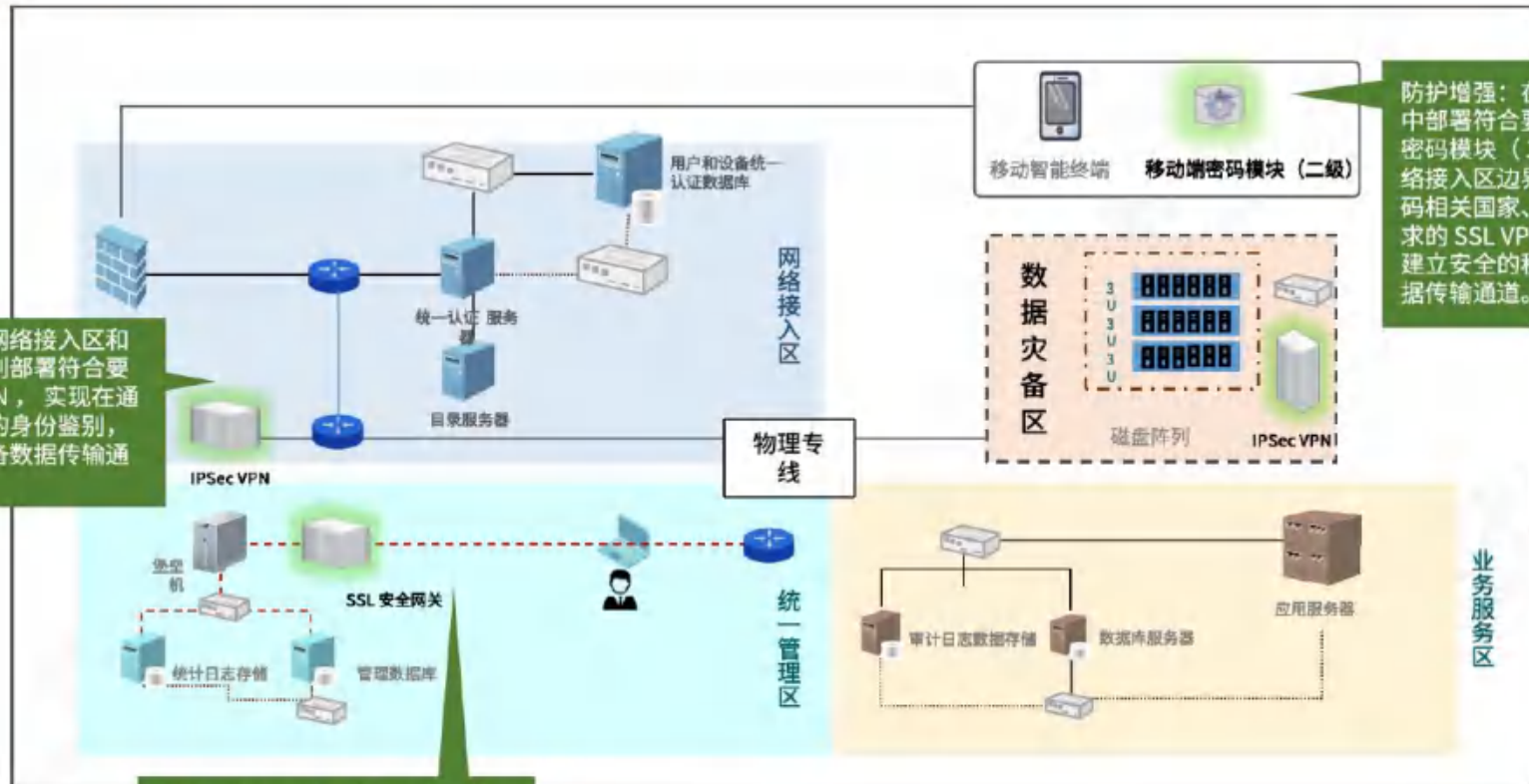
风险：存在通信数据在信息系统外部被非授权截取、非授权篡改风险。

问题：通信前未使用密码技术对通信双方进行验证，未使用密码技术对灾备数据传输通道进行机密性和完整性保护；

风险：存在非法设备从外部接入内部网络\通信数据在信息系统外部被非授权截取、非授权篡改风险。

需求：身份鉴别，访问控制信息完整性

网络和通信安全防护示例



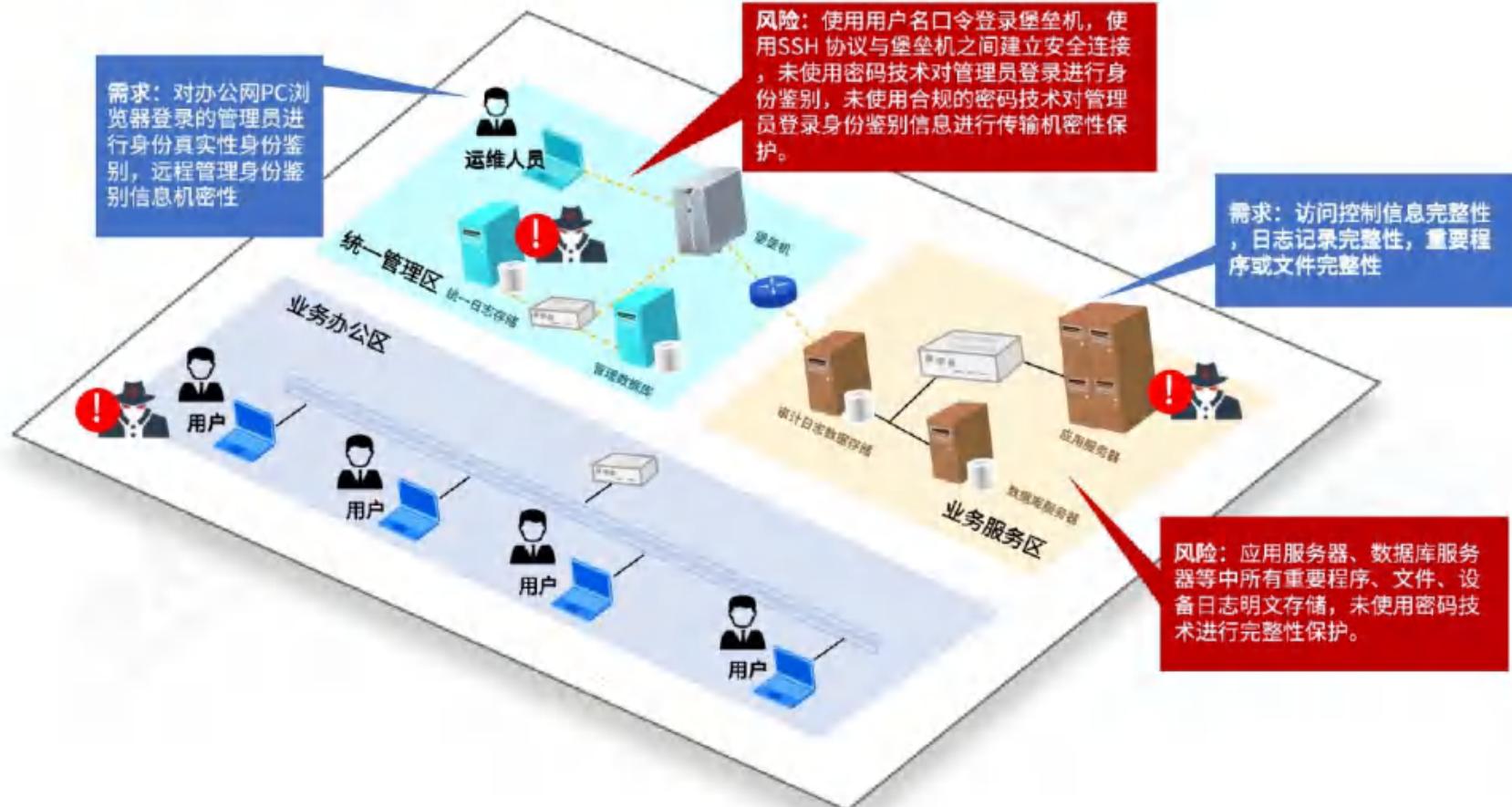
防护增强：在网络接入区和数据灾备区分别部署符合要求的IPSec VPN，实现在通信前通信双方的身份鉴别，建立安全的灾备数据传输通道。

防护增强：在移动端App中部署符合要求的移动端密码模块（二级）、在网络接入区边界部署符合密码相关国家、行业标准要求的SSL VPN安全网关，建立安全的移动端App数据传输通道。

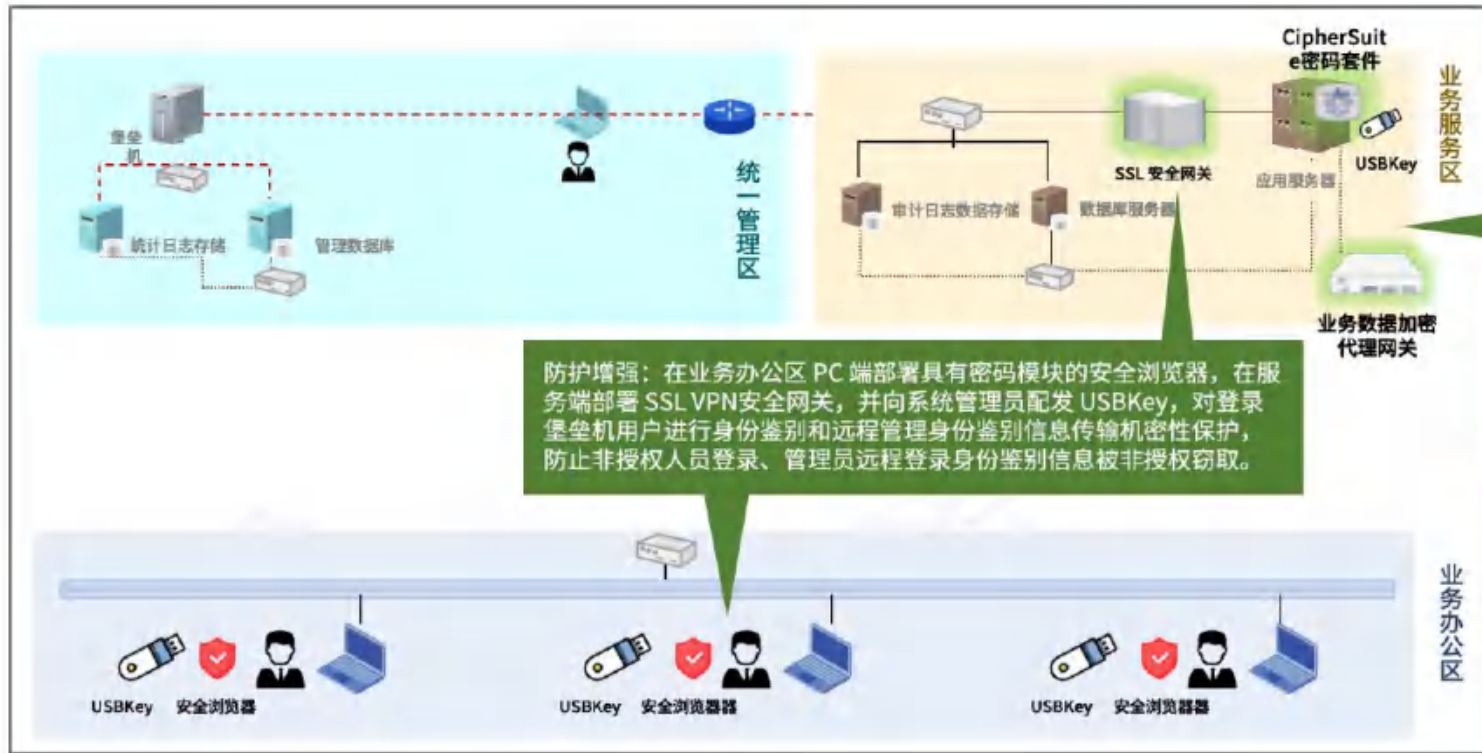
防护增强：在统一管理区部署符合密码相关国家行业标准要求的SSL VPN安全网关，建立安全的集中管理通道。

(3) 设备和计算安全

设备和计算安全风险分析与密码需求



设备和计算安全防护示例

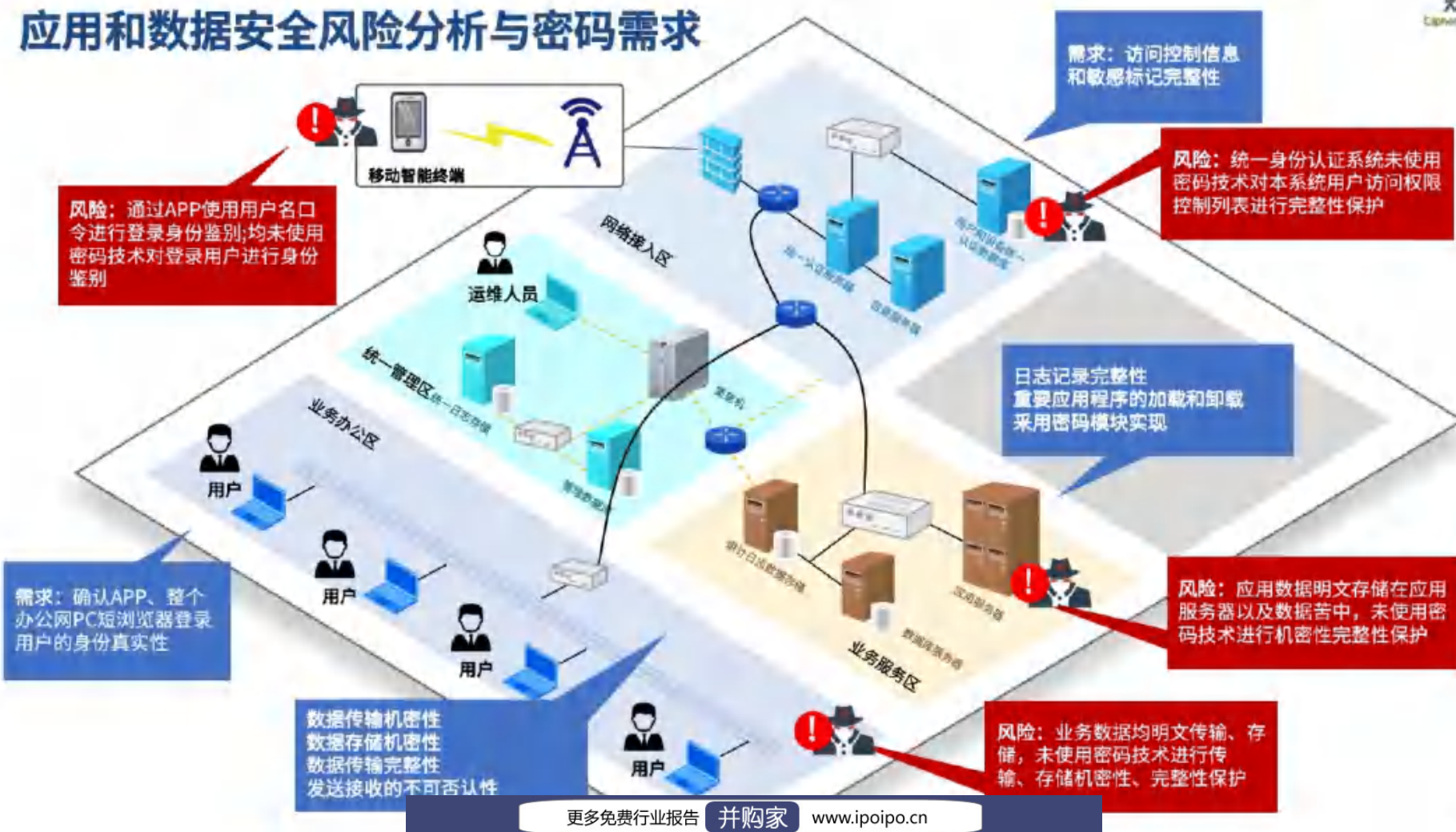


防护增强：在业务服务区部署符合标准要求的CipherSuite密码套件、业务数据代理加密网关与USBKey对所有重要程序或文件、设备日志在生成时通过调用服务器密码机进行完整性保护，使用或读取这些程序和文件时，通过USBKey进行验签以确认其完整性；公钥存放在USBKey中。

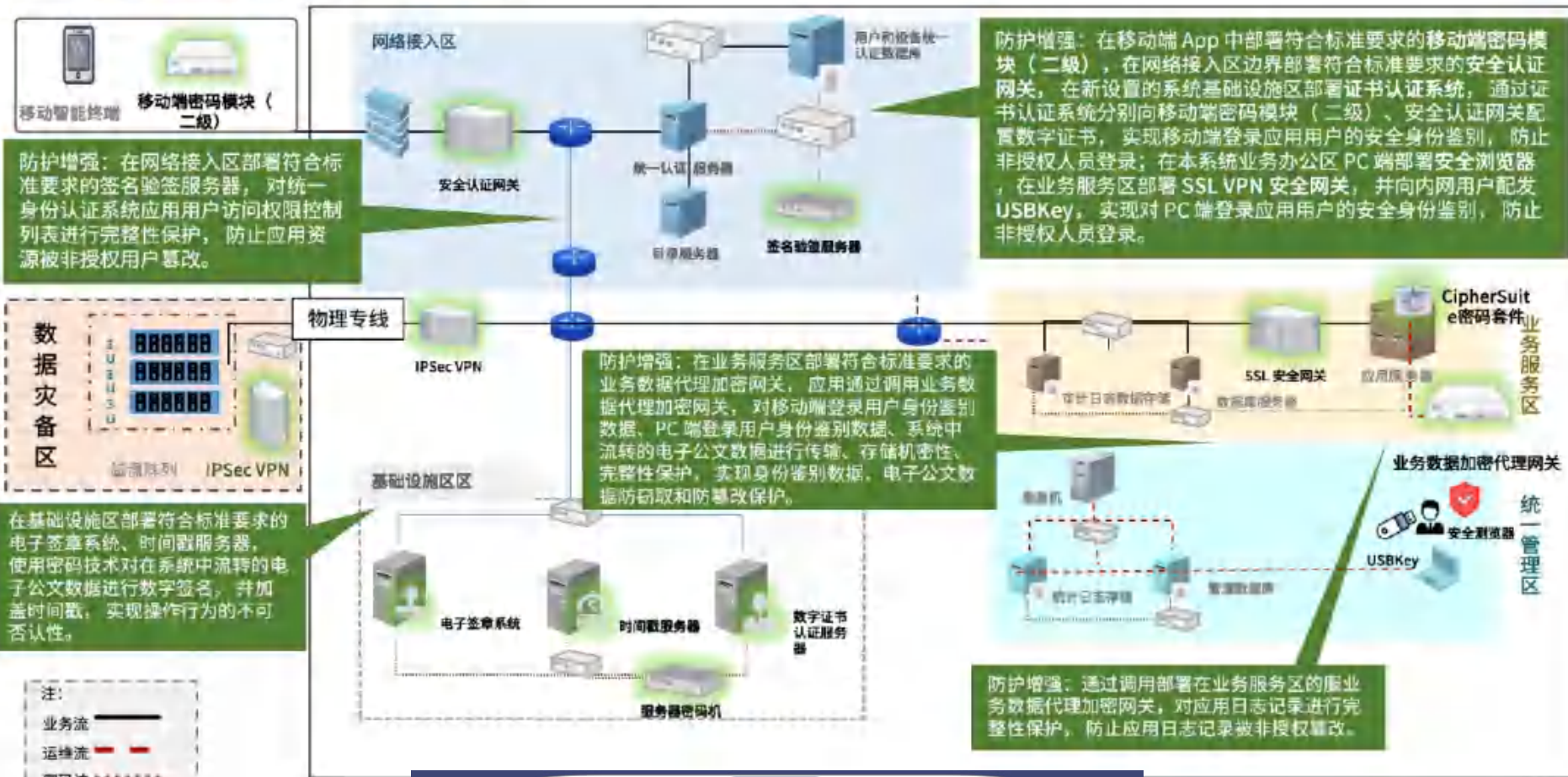
企业办公楼一层机房

(4) 应用和数据安全

应用和数据安全风险分析与密码需求

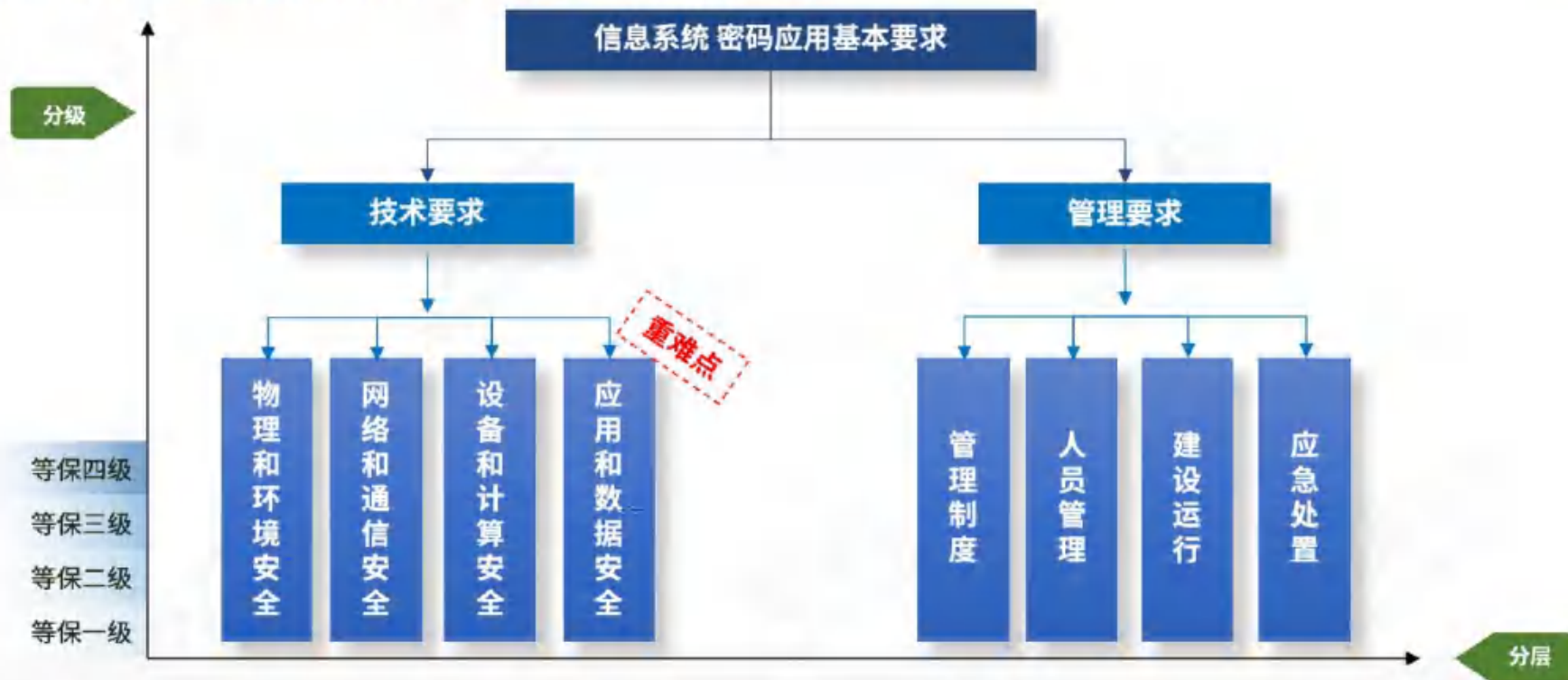


应用和数据安全防护示例



炼石密改方案优势

密评合规：免改造技术解决密评改造痛点



评估原则

遵循商用密码管理政策和GB/T39786-2021《信息系统密码应用基本要求》、《信息系统密码测评要求》等相关密码标准的要求，遵循独立客观、公正原则。

评估内容

主要对物理和环境、网络和通信、设备和计算、应用和数据四个技术层面，以及管理制度、人员管理、建设运行、应急处置四个管理层面进行测评。

敏捷实施：数据加密脱敏一体化

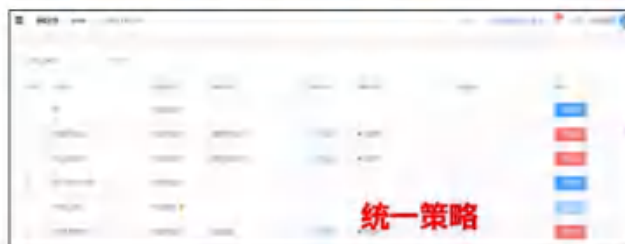
存储

使用

加工

传输

管理



配置

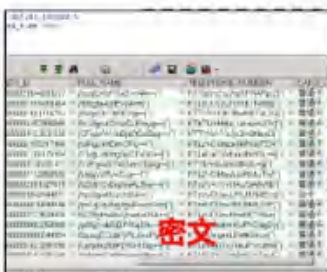
CASB数据安全平台

集中管控

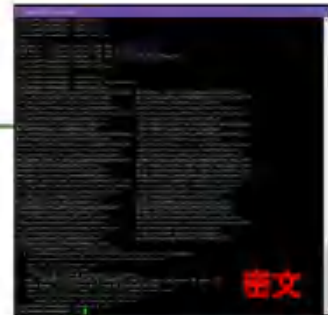
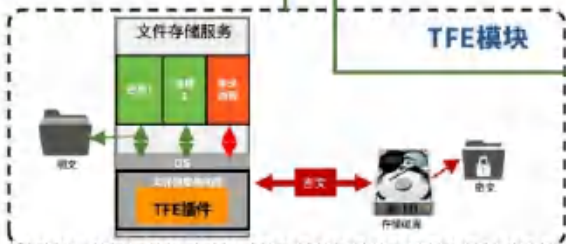
密钥和安全策略

脱敏数据

名称	格式	所有者	最后修改
表1	2114	张明	2020-01-24 09:05
表2	2142	李华	2020-01-24 09:05
表3	8402	王强	2020-01-24 09:05
表4	1100	赵刚	2020-01-24 09:05
表5	2885	陈伟	2020-01-24 09:05
表6	4605	孙磊	2020-01-24 09:05
表7	5505	周涛	2020-01-24 09:05

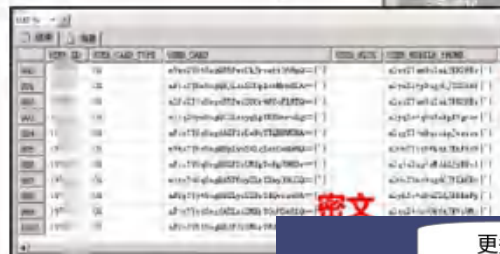


AOE-Plugin模块



业务应用

应用集成SDK



AOE-Proxy模块



高性能：PCT专利保护的高速国密实现，不影响业务效率

基于PKI的数字信封加密

协同签名身份鉴别

密钥派生接口

EVP国密接口

FPE格式保留加密



SM2

SM3

SM4

SM9

ZUC



基于SM4的保留格式加密（FPE）

加密10亿条手机号，仅耗时20秒



2018年保密技术交流会暨产品博览会
Information Security Technology Conference & Expo 2018



天下密码
唯快不破

炼石独有PCT专利
打破Intel垄断

单颗CPU上SM4加解密
突破 140Gbps!

相当于每秒可加密6部3GB大小的高清电影

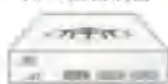
移动端SM4加解密
突破1.7Gbps!

相当于每秒可加密100多张2MB大小的高清照片



高可靠：专业密钥管理、实时离线解密，保障高可用

KMS密管设备



真随机数

根密钥

- 1、根据门限算法加密导出至3个USBKey，任意2个可还原
- 2、跨设备需人工同步

真随机数

模块密钥

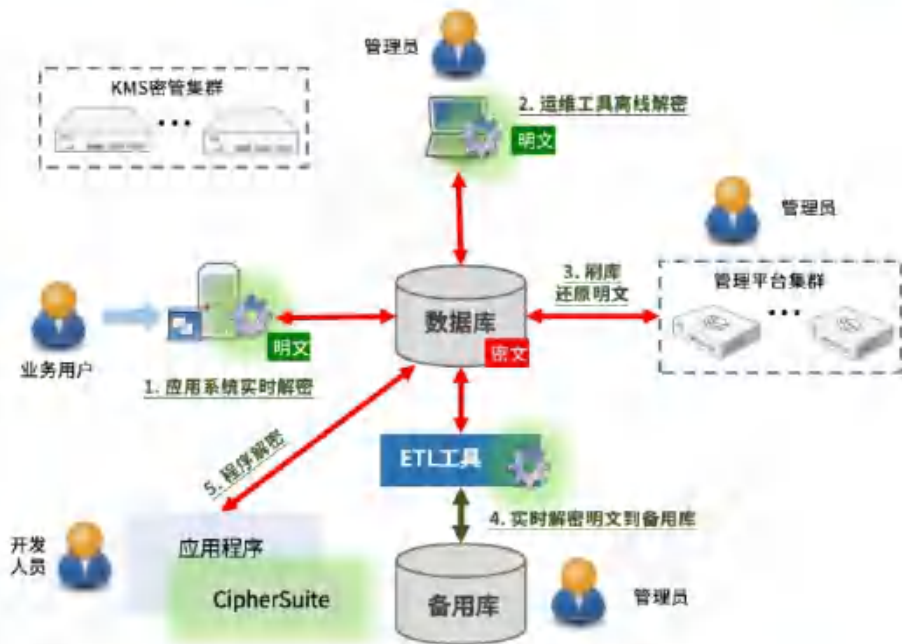
- 1、由根密钥加密落盘存储
- 2、跨设备自动同步

模块密钥
派生

工作密钥（数据加密、数据MAC）

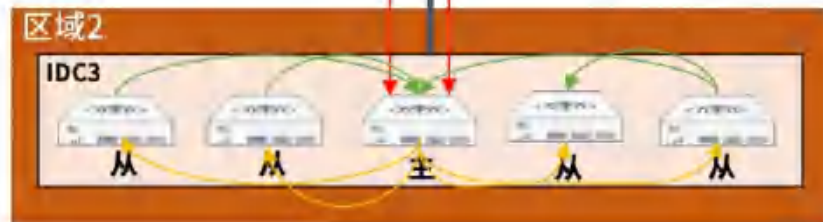
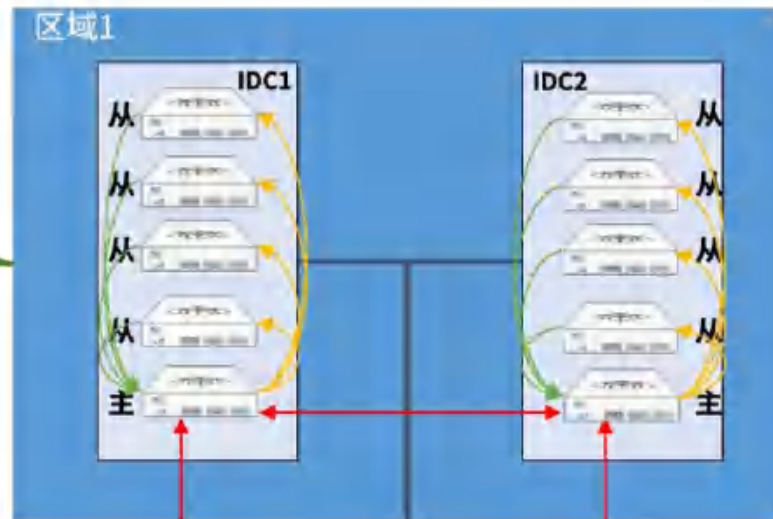
- 1、不落盘存储
- 2、由模块密钥实时派生

- 密管设备**支持双机热备、两地三中心等高可用模式**，根密钥明文不出密码卡，模块密钥明文不出密管设备
- **工作密钥安全从平台分发到数据控制面模块，模块可缓存工作密钥后独立运行**，平台不需要实时在线
- 保守策略下，当重启应用服务后，模块才需从平台更新密钥



- 密码算法是标准，密钥管理机制可靠，**只要密文数据还在，一定可解密**
- 常态状态下，支持应用系统解密、支持DBA运维工具直接解密
- 应急情况下，支持刷库还原明文、支持实时解密明文到备用库
- 极端情况下，用运维工具或程序可以兜底解密

高可用：模块健壮可诊断、平台“两地三中心”



【模块可离线运行】

- 模块从平台获取规则后可缓存在内存中，当平台不可用也可正常运行
- 仅当模块所在服务重启时才需要从平台集群重取规则

【模块强化健壮性】

- 以AOE插件为例，本身作为应用的一部分，无单独进程，不会死进程
- 在没有匹配规则状态下，模块默认采用透传模式，最大限度优先业务
- 模块经过多年研发打磨、运行实践，兼容广泛苛刻的企业级应用场景

【模块可诊断】

- 模块自身可记录环境、启动流程、异常事件等日志，以及告警功能
- 针对Java等应用环境支持不停机实时诊断机制，排查潜在故障成因

- 两地三中心各5套安全管理平台（以及KMS）组成集群，三中心的主之间实时双向同步数据，在同一中心内主从间同步数据

高安全：灵活密码模块满足高等级合规要求

硬件密码机/密码卡
提供密码算力

符合GB/T 39786等保
四级要求，性能较低

应用系统CPU
提供密码算力

符合GB/T 39786等保
三级要求，且性能高

免改造加密模块

硬件密码机/卡

加解密算力提供

密钥管理

应用系统CPU

免改造安全模块

应用系统部署免改造模块，调用硬件密码机/密码卡算力实现加解密

硬件密码机

密钥管理

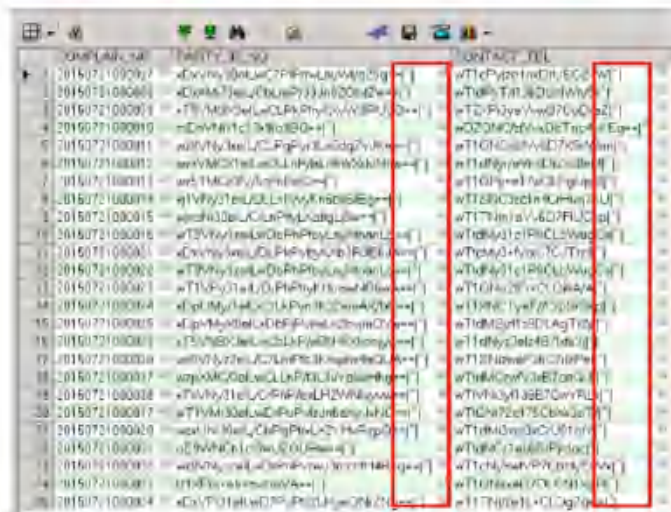
应用系统CPU

加解密算力提供

免改造安全模块

应用系统部署免改造安全模块，调用本地CPU算力实现加解密

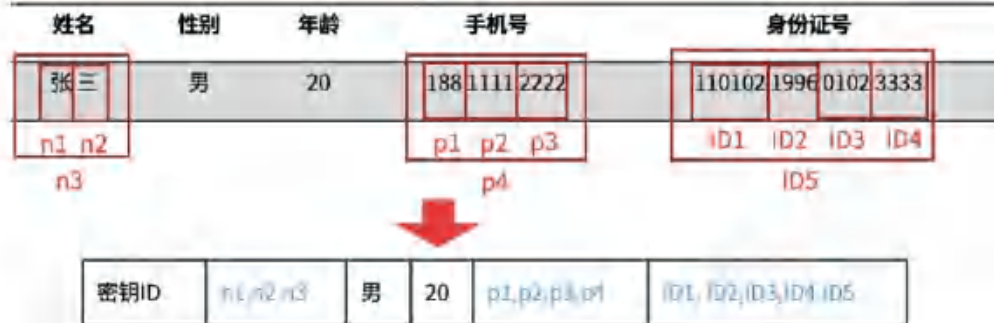
明密文标识确保加解密可靠



- 炼石产品加密后，会在密文中添加密文标识，可保证明文不会被二次解密，密文不会被二次加密
- 在加密功能上线过程中，不可避免会出现明密文混合的情况，可通过明密文标识将明文和密文区分开

支持数据加密后的密文态查询

类型	规则	示例
a	手机号型	按照3、4、4拆分加密
b	身份证号型	按照6、4、4、4拆分加密
c	住址型	按照3、3、其余拆分加密
e	其他	



- 支持密态数据库的模糊查询操作。对加密字段做特定处理，先将加密字段按照规则拆解，然后对拆解后部分分别加密处理，之后将各部分密文合成一个字段（拆解的规则可由应用定制化，通过策略管理来进行配置）
- 限制条件
 - 支持应用对加密策略进行定制，但加密策略确定后原则上不建议更改
 - 为支持模糊查询会对加密字段的长度进行扩张

国密合规场景：一站式密改套餐敏捷交付

序号	测评项	测评单元	权重 (3级)	备注	约束	得分		
1	物理和环境安全 10分	身份鉴别	1	高风险	宜	10分	10分	
2		电子门禁记录数据存储完整性	0.7		宜			
3		视频记录数据存储完整性	0.7		宜			
4	网络和通信安全 20分	身份鉴别	1	高风险	应	≥10分	≥18分	
5		通信数据完整性	0.7		宜			
6		通信过程中重要数据的机密性	1	高风险	应			
7		网络边界访问控制信息的完整性	0.4		宜			
8		安全接入认证	0.4		可			
9	设备和计算安全 10分	身份鉴别	1	高风险	应	≥5分	≥8分	
10		远程管理通道安全	1	高风险	应			
11		系统资源访问控制信息标记完整性	0.4		宜			
12		重要信息资源安全标记完整性	0.4		宜			
13		日志记录完整	0.4		宜			
14		重要可执行程序完整性、重要可执行程序来源真实性	0.7		宜			
15	应用和数据安全 30分	身份鉴别	1	高风险	应	≥20分	≥26分	
16		访问控制信息完整性	0.4		宜			
17		重要信息资源安全标记完整性	0.4		宜			
18		重要数据传输机密性	1	高风险	应			
19		重要数据存储机密性	1	高风险	应			
20		重要数据传输完整性	0.7		宜			
21		重要数据存储完整性	0.7	高风险	宜			
22		不可否认性	1	高风险	宜			
23	安全管理 30分	管理制度、人员管理、建设运行、应急处理			预估		≥25分	≥28分
						≥70	≥90	

90+分套餐

70+分套餐

视频监控安全一体机
国密门禁系统
VPN网关
密钥管理与数据加密及认证平台
服务器密码机
软件密码模块
密码卡
USBKey

+

签名验签服务器
时间戳服务器
安全认证网关
证书认证系统
电子签章系统
国密浏览器

数据安全实战防护场景

基于产品与服务，事前事中事后全防护

炼石客户交付：1平台、2价值、3阶段、4指标、5能力

炼石数据安全交付体系

免改造数据安全主平台

数据安全模块管理 行业敏感数据模板 个人敏感数据模板 数据安全事件调度 数据安全策略下发 数据资产视图 数据安全监控中心

内在风险防护

外部人员

防范外部黑客恶意攻击窃取
防范外部合作伙伴越权使用
防范供应链数据滥用
防范竞争对手恶意数据篡改

内部人员

防范运维人员违规操作
防范业务人员越权访问
监测业务人员风险操作
追溯业务人员数据泄露



外部合规遵循

四法

《网络安全法》
《密码法》
《数据安全法》
《个人信息保护法》

四例

《网络安全等级保护条例》（征）
《关键信息基础设施安全保护条例》
《商用密码管理条例》
《网络数据安全管理条例》（征）

等保
关保
密评
数评

贯穿数据安全建设

数据安全规划（服务）

数据安全建设（产品+服务）

数据安全运营（服务）

多

兼容多
适应广泛应用架构

快

交付快
免改造应用增强数据安全

好

防护好
覆盖事前事中事后

省

省成本
降低总体拥有成本(TCO)

数据资产管理能力

数据资产目录 数据识别管理
用户身份视图 自动化分类分级
敏感数据识别 数据标注
数据风险评估 数据血缘分析
数据内容合规 数据脱敏

数据主动防护能力

数据库加密 文件级加密 加密备份恢复
数据脱敏 TDF 可信数据格式 TEE 可信执行环境
去标识化 数据信封 数据完整性
终端/网络DLP 数据加密 数据沙箱

数据风险检测能力

业务漏洞检测 数据访问检测
API敏感风险 业务风控
数据流转检测 DBSA
网络流量分析 交换机端口监测

数据风险响应能力

事件追溯处置
威胁响应接口
内容/端口阻断
攻击定位

数据审计追溯能力

数据访问留存 数据库审计
文件访问审计 数据库访问审计
数据水印 屏幕水印
操作管理 元数据标注
接口审计 数据流追溯

体系化数据安全治理

数据安全三年提升规划
安全建设现状分析报告
数据安全政策治理报告
数据安全体系参考架构

场景化数据安全建设

政务数据交换共享安全保障
金融个人信息安全防护建设
数评/密评安全合规建设
数据跨境安全合规方案

单项产品能力支撑

数据资产管理系统
数据加密脱敏系统
数据检测响应系统
数据安全审计系统

产品体系：免改造平台灵活交付多重安全能力，易部署易扩展



免改造应用敏捷交付

无需改动目标应用系统的代码，即可为各行业应用系统增强数据加密、脱敏、审计保护能力

适应复杂应用架构

有效兼容各行业的广泛应用架构，如JAVA、C等主流开发语言、兼容开放协议的关系型数据库和非关系型数据库、兼容Linux/信创OS/Windows等

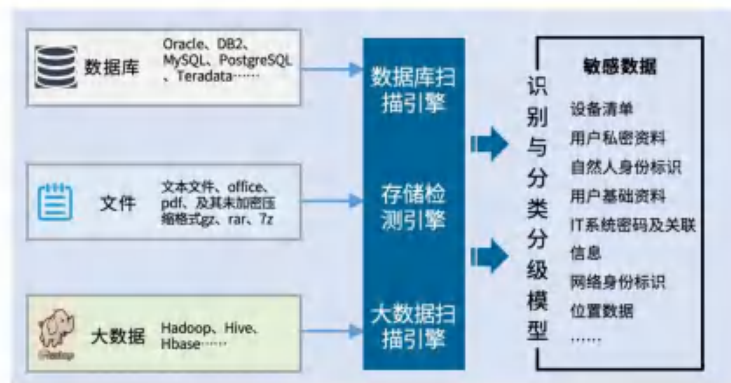
集中式管控分布式保护

引入批量应用系统的“集中式管控，分布式保护”体系，自上到下的全层级部署管控

高性能国密保障效率

具备PCT国际专利保护的高性能国密技术，在单颗X86 CPU上实现SM4加解密速度突破**140Gbps**

数据可见：数据分类识别，为分级管控打基础



事前防护：最小化敏感数据访问范围

存储 使用 加工 传输 销毁

易于实施的“主体到人”，支持与应用身份管理打通



- 可适配应用系统自带身份管理或统一IAM系统，实现结合用户身份的动态脱敏
- 可支持ABAC基于属性的访问控制等细粒度授权

域内数据：存储加密、使用解密/脱敏

存储

使用

加工

传输

结构化数据

支持ABAC的访问控制策略，
实现用户与字段文档级防护

主体到人

客体到字段

细粒度
访问控制

应用服务器

数据库

AOE插件

AOE代理

窃取数据

面向用户侧动态脱敏

面向服务端存储加密

密钥管理系统 数据安全管理平台

非结构化数据

TFE文件安全模块

FDE全磁盘加密



不影响业务人员使用、不影响DBA运维

示例

姓名	年龄	性别	职业
张三	25	男	程序员
李四	30	女	产品经理
王五	35	男	市场经理
赵六	40	女	财务总监
钱七	45	男	CEO

应用查看脱敏后数据

示例

姓名	年龄	性别	职业
张三	25	男	程序员
李四	30	女	产品经理
王五	35	男	市场经理
赵六	40	女	财务总监
钱七	45	男	CEO

应用看到密文

示例

姓名	年龄	性别	职业
张三	25	男	程序员
李四	30	女	产品经理
王五	35	男	市场经理
赵六	40	女	财务总监
钱七	45	男	CEO

DBA工具查看脱敏数据

示例

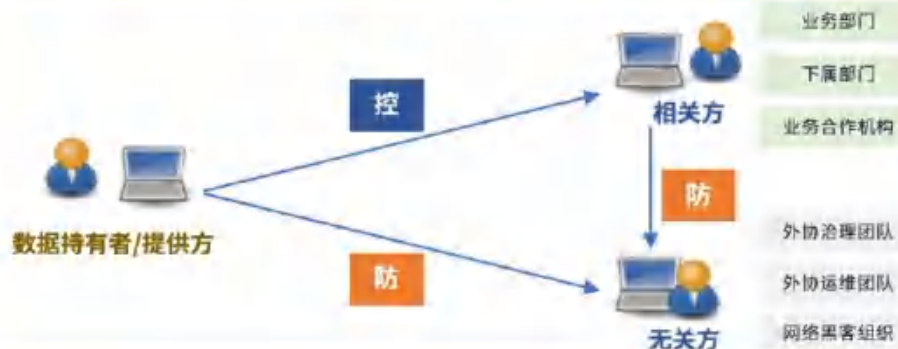
姓名	年龄	性别	职业
张三	25	男	程序员
李四	30	女	产品经理
王五	35	男	市场经理
赵六	40	女	财务总监
钱七	45	男	CEO

DBA工具查看密文

跨域数据：轻改造落地“数据可见不可转”

存储 → 使用 → 加工 → 传输 → 提供

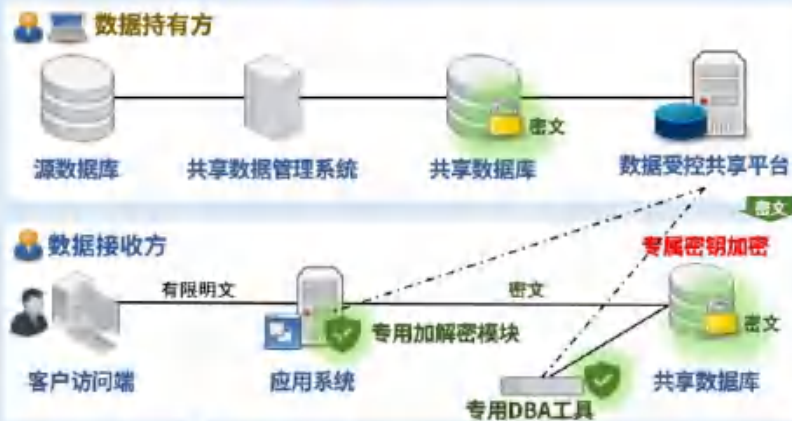
公开/删除
提供
传输
加工
使用
存储
收集



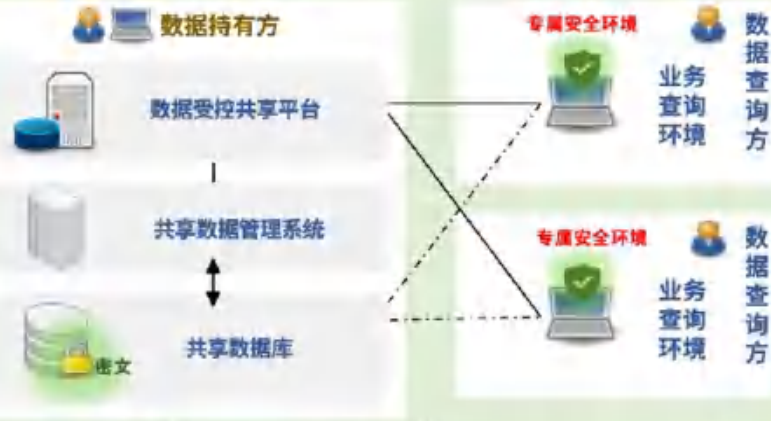
数据已成为企业间可以交易的商品，但交易后存在“数据失控”问题困扰着数据持有者：

- 数据的接收方有没有对数据进行滥用？
- 对方有没有再次将数据外发给第三方？
- 这些数据在接收方的有效期如何控制？

1. 离线场景：实现数据可见不可转



2. 在线场景：实现数据可查不可转



I.识别

P

更多免费行业报告

并购买

www.ipopo.cn

恢复

C.反制

387

事中检测：SQL注入攻击防御

- 在AOE-Plugin、AOE-Proxy等模块中，可根据内置或自定义规则识别风险SQL语句
- 针对风险SQL可做实时告警或实时阻断



规则项	描述
selectWhereAlwaysTrueCheck	检查SELECT语句的WHERE子句是否是一个永真条件
selectHavingAlwaysTrueCheck	检查SELECT语句的HAVING子句是否是一个永真条件
deleteWhereAlwaysTrueCheck	检查DELETE语句的WHERE子句是否是一个永真条件
deleteWhereNoneCheck	检查DELETE语句是否无where条件，这是有风险的，但不是SQL注入类型的风险
updateWhereAlwaysTrueCheck	检查UPDATE语句的WHERE子句是否是一个永真条件
updateWhereNoneCheck	检查UPDATE语句是否无where条件，这是有风险的，但不是SQL注入类型的风险
conditionAndAlwaysTrueAllow	检查查询条件(WHERE/HAVING子句)中是否包含AND永真条件
conditionAndAlwaysFalseAllow	检查查询条件(WHERE/HAVING子句)中是否包含AND永假条件
conditionLikeTrueAllow	检查查询条件(WHERE/HAVING子句)中是否包含LIKE永真条件
conditionOpXorAllow	查询条件中是否允许有XOR条件。XOR不常用，很难判断永真或者永假，缺省不允许。
conditionOpBitwiseAllow	查询条件中是否允许有"&"、"^"、" "、"~"运算符。
conditionDoubleConstAllow	查询条件中是否允许连续两个常量运算表达式
minusAllow	是否允许SELECT * FROM A MINUS SELECT * FROM B这样的语句
intersectAllow	是否允许SELECT * FROM A INTERSECT SELECT * FROM B这样的语句
constArithmeticAllow	拦截常量运算的条件。比如说WHERE FID = 3 - 1，其中"3 - 1"是常量运算表达式。
---	---

示例



Select * from table where id=**1** and Field like '%**keyword**%' and tid in(**1,2,3**) order by **Field** desc

事中检测：业务人员风险操作监测

管理 使用 加工 决策 评估



用户C

应用



数据库



示例

用户C 20161221 23:43:22 下载文件 产品库/
详细设计/ 作动器总体设计图（最终）
行为不符合日常工作时间 行为异常 执行阻断

场景举例

某员工用户C有权使用单位的PLM系统，并能访问到某Z型产品中的设计数据。偶然一次，此人在正常工作时间内，批量下载全套的产品数据，此时数据控制面的实时监控功能捕捉到此异常行为，会立即执行阻断，并将该事件进行记录和报警。

- 免改造控制面对所有流经的业务操作进行监测，结合当前的业务上下文，判断行为是否符合正常的行为模式
- 如果发现是异常操作和不合规操作，则进行告警甚至对操作阻断，以防止恶意操作带来的数据泄露和系统破坏

示例

客户信息安全内控增强

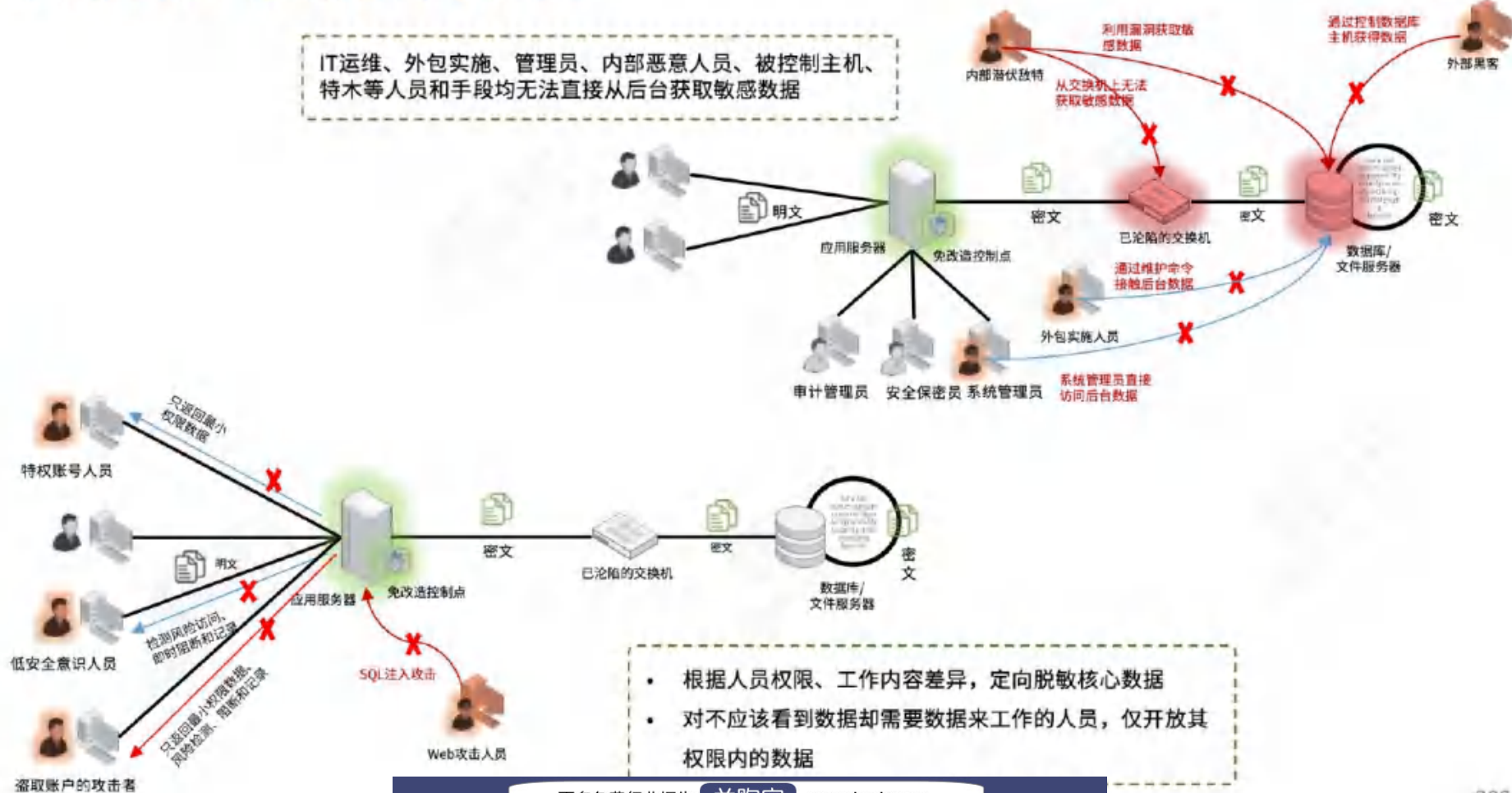
- 客服人员每天需要查询高价值的大客户信息，以便提供服务，但存在过量访问的内控风险，而业务应用往往缺失细粒度安全机制
- 通过免改造控制面的安全内控增强，可实现客服人员每天访问大客户信息的阈值，比如100条以内可正常访问，超过100条系统进行告警，超过200条会触发阻断（通过流程审批后才能访问）

敏捷部署：旁路平台结合主路控制点，免改造应用落地数据识别与保护



实战对抗：有效防护内外威胁

IT运维、外包实施、管理员、内部恶意人员、被控制主机、特木等人员和手段均无法直接从后台获取敏感数据



炼石免改造数据安全实现“一实战、双合规”

实战是检验安全能力的唯一标准

实战对抗

HWV攻防演练

网络攻破后数据不泄露

形成实战
最佳实践

将偶发的、高技术水平的对抗风险，
转化成常态的、可重复验证的非对抗风险



对抗

实战之三体



密评

过程合规

商用密码应用安全性评估

敏捷交付国密合规改造



结果合规

数据安全能力成熟度认证

数据安全管理体系认证

个人信息保护认证

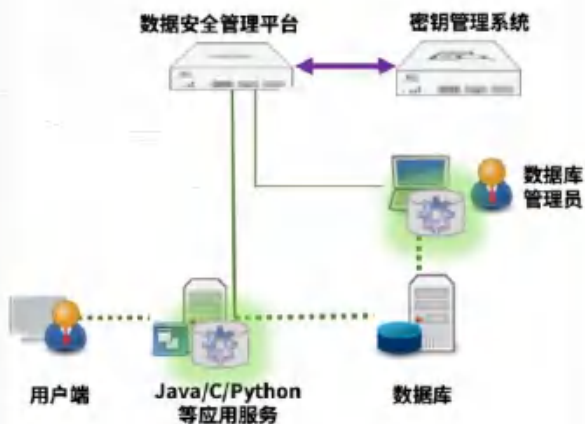
数据安全风险评估

方案优势：兼容多、交付快、防护好

适应大多数企业应用架构



免改造应用敏捷实施



覆盖事前事中事后的防绕过保护机制



通过调研和梳理业务系统主要数据流转和核心应用功能,建立数据流向清单和数据应用清单,配合炼石自研数据资产扫描工具,提供全景化动态化数据分类分级服务。



风险呈现

Figure 1 illustrates the Data Security Dynamic Risk Quantification Presentation. It shows a process flow from Value Identification to Risk Identification, then to Risk Evaluation, and finally to Risk Response. The central part of the diagram is a table titled 'Reference Data Security Standard Construction and Risk Evaluation Model' (参考数据安全标准构建及风险评估模型). The table lists various data types and their associated risks, categorized by Data Type (数据类型), Data Source (数据来源), Data Flow (数据流), Data Storage (数据存储), and Data Use (数据使用). The Risk Evaluation (风险评估) column uses a color-coded scale (Low Risk, Medium Risk, High Risk) to indicate the level of risk. The Risk Response (风险处置) column shows the corresponding response level (High Risk, Medium Risk, Low Risk).

01 操作审计

02 合规审计

Figure 1 illustrates the overall framework for integrating cryptographic standards. At the top, the process flows from 'Cryptographic Standard Integration' to 'Cryptographic Product' and 'Cryptographic Tools'. Below this, 'Cryptographic Product' is linked to 'Cryptographic Technology Integration' and 'Cryptographic Technology Consultation'. 'Cryptographic Tools' is linked to 'Cryptographic Evaluation and Testing'. The bottom section details 'Cryptographic Technology Consultation' and 'Cryptographic Evaluation and Testing' with various sub-processes and icons.

炼石专项服务1-分类分级服务

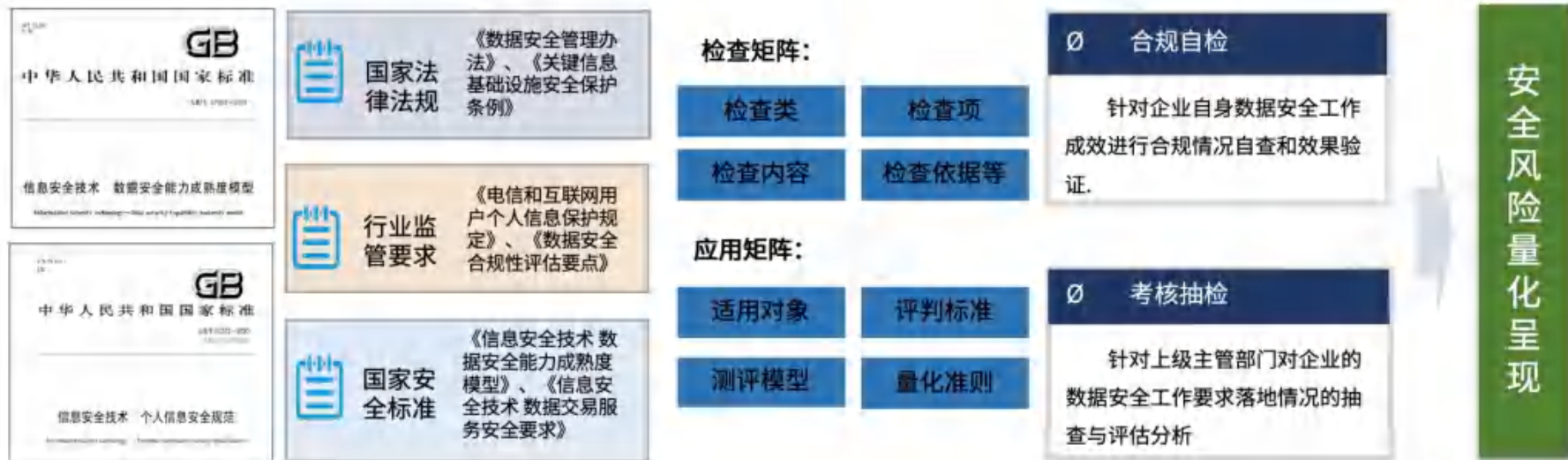
通过调研和梳理业务系统主要数据流转和核心业务应用功能，逐步建立数据流向清单和数据应用清单，配合炼石自研数据资产扫描工具，为政企客户数据资产管理提供全景化动态化数据分类分级服务。



炼石专项服务2-合规检查服务

合规评估围绕数据全生命周期管理，根据用户系统数据资产重要程度及安全需求，对数据安全现状、技术管控能力进行评估。评估内容包括机构人员建设情况、基本制度完善情况、技术能力保障情况、数据全生命周期管控情况四个方面。

法律法规、监管要求 → 规则细化 → 落地评估 → 风险呈现



针对敏感数据安全，建立审计实施体系，完善审计流程，开展审计项开展定期审计工作。

运营管埋
风险监测

安全技术
风险监测

组件基线 风险监测

7大类21个子项115个风险点

9大类37个事项71个风险点

10类组件9大类控制项79个风险点

基础设施风险监测

物理环境与机房安全、云基础设施安全

网络系统风险监测

網絡安全、系統安全、
大數據平台組件安全

业务应用风险监测

不良信息管控、Web应用安全防护

数据采集风险监测

采集终端接入安全、数据采集行为安全、敏感数据采集安全、采集数据传输安全、异常采集行为告警

数据存储风险监测

数据加密存储、存储空间隔离、数据残留与销毁、数据存储访问控制、数据封装、大数据备份与恢复、数据完整性保护

数据处理风险监测

计算环境安全、敏感数据处理安全、数据使用访问控制

平台接口风险监测

平台内部传输安全、平台内部接口安全、平台对外接口安全

平台安全风险监测

管理平台安全、4A及金库管
控安全、安全事件管理、灾
难恢复、日志审计、安全高
效感知和监测预警

应用支撑风险监测

应用接入安全、认证授权、应用异常行为检测(增强)、数据脱敏、数据关联性隔离(增强)、数据转移安全

根据敏感数据识别台账，结合各业务系统影响数据安全的威胁、漏洞变化趋势。并参照信息安全风险评估模型，从数据的重要性、脆弱性和威胁性三要素计算敏感数据、业务系统的风险值。



炼石专项服务4-安全审计服务

针对敏感数据安全，建立审计实施体系，完善审计流程，开展审计项开展定期审计工作。

目的：通过对关键数据操作审计，重点检查数据操作过程的合规情况，并借助分级审计机制提高审计效率。



目的：通过合规审计，由专业审计团队执行，重点检查数据安全流程和工作的执行情况。

关键数据操作审计



- ☐ 页面查询、导出、修改、下载
- ☐ 数据库查询、导出、修改、删除、下载
- ☐ 文件查询、导出、修改、

配置变更审计



- ☐ 关键服务启停
- ☐ 修改、删除日志配置
- ☐ 关键参数修改、删除
- ☐ 其他影响数据安全配置

账号权限操作



- ☐ 账号申请、使用、变更、删除
- ☐ 权限申请、变更、删除

对外数据接口审计



- ☐ 接口访问
- ☐ 接口使用
- ☐ 接口配置变更

金库审计



- ☐ 审批情况
- ☐ 审批结果
- ☐ 使用情况

数据第三方审计



- ☐ 保密协议签订情况
- ☐ 资质背景
- ☐ 人员和技术能力

数据服务使用审计



- ☐ 数据用途
- ☐ 数据使用场景
- ☐ 数据应用范围

炼石专项服务5-个人信息安全影响评估服务

国家标准《信息安全技术 个人信息安全规范》中的相关要求



个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄露、损毁、丢失。

炼石免改造数据安全



www.ciphergateway.com



010-88459460



sales@ciphergateway.com

更多免费行业报告

并购家

www.ipopo.cn