

图解

《国家密码管理局商用密码随机抽查事项清单》 (2024年版)

炼石网络
2024年7月

1. 《国家密码管理局商用密码随机抽查事项清单（2024年版）》

2. 抽查依据中涉及的相关法规解读

01 《密码法》

02 《商用密码管理条例》

03 《商用密码检测机构管理办法》

04 《商用密码应用安全性评估管理办法》

3. 炼石免改造数据安全性与密码应用实践



《国家密码管理局商用密码随机抽查事项清单（2024年版）》发布

**国家密码管理局**
WWW.SCA.GOV.CN

请输入关键词

热门搜索: 商用密码 电子认证 电子签名

首页 | 机构概况 | 新闻动态 | 信息公开 | 在线服务 | 互动交流 | 专题专栏

首页 > 新闻动态 > 通知公告

国家密码管理局

关于发布《国家密码管理局商用密码随机抽查事项清单（2024年版）》的公告

发布日期: 2024-07-19 来源: 国家密码管理局

【字体: 大 中 小】  打印

国家密码管理局公告
(第 47 号)

根据《中华人民共和国密码法》、《商用密码管理条例》及相关商用密码管理规章,现发布《国家密码管理局商用密码随机抽查事项清单(2024年版)》,自发布之日起施行。2018年7月7日发布的《国家密码管理局关于印发商用密码随机抽查事项清单的通知》(国密局字〔2018〕268号)同时废止。

附件:国家密码管理局商用密码随机抽查事项清单(2024年版)

国家密码管理局
2024年7月19日

2024年7月19日,根据《中华人民共和国密码法》、《商用密码管理条例》及相关商用密码管理规章,国家密码管理局发布《国家密码管理局商用密码随机抽查事项清单(2024年版)》,自发布之日起施行,2018年7月7日发布的《国家密码管理局关于印发商用密码随机抽查事项清单的通知》(国密局字〔2018〕268号)同时废止。

国家密码管理局商用密码随机抽查事项清单（2024年版）

商用密码产品检测随机抽查

01

商用密码应用安全性评估随机抽查

商用密码应用随机抽

电子认证服务使用密码随机抽查

电子政务电子认证服务随机抽查

序号	抽查类别	抽查事项	抽查内容	抽查依据	抽查主体	抽查对象	抽查比例和频次	抽查方式
1	商用密码检测	商用密码产品检测随机抽查	符合资质认定条件和要求、遵守从业规范、开展商用密码产品检测活动、实施标准等情况	《中华人民共和国密码法》第二十五条、第三十五条 《商用密码管理条例》（国务院令760号）第十三条、第十四条、第十六条、第四十七条、第五十一条 《商用密码检测机构管理办法》（国家密码管理局令第2号）第三条、第五条、第六条、第十二条、第十三条、第十四条、第十五条、第十六条、第十七条、第十八条、第十九条、第二十条、第二十一条、第二十二条、第二十三条、第二十五条、第二十六条	密码管理部门	商用密码检测机构（商用密码产品检测业务）	- 在商用密码检测机构（商用密码产品检测业务）名录中随机抽取。 3年内已接受随机抽查、无违法违规行为的，不列入随机抽查范围。 - 对随机抽查不合格的机构加大抽查频次。	现场、书面、网络检查相结合

国家密码管理局商用密码随机抽查事项清单（2024年版）

商用密码产品检测随机抽查

商用密码应用安全性评估随机抽查

商用密码应用随机抽

电子认证服务使用密码随机抽查

电子政务电子认证服务随机抽查

02

序号	抽查类别	抽查事项	抽查内容	抽查依据	抽查主体	抽查对象	抽查比例和频次	抽查方式
2	商用密码检测	商用密码应用安全性评估随机抽查	符合资质认定条件和要求、遵守从业规范、开展商用密码应用安全性评估活动、实施标准等情况	《中华人民共和国密码法》第二十五条、第三十五条 《商用密码管理条例》（国务院令760号）第十三条、第十四条、第十六条、第四十七条、第五十一条 《商用密码检测机构管理办法》（国家密码管理局令第2号）第三条、第五条、第六条、第十二条、第十三条、第十四条、第十五条、第十六条、第十七条、第十八条、第十九条、第二十条、第二十一条、第二十二条、第二十三条、第二十五条、第二十六条 《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）第四条、第十条、第十一条	密码管理部门	商用密码检测机构 （商用密码应用安全性评估业务）	- 在商用密码检测机构（商用密码应用安全性评估业务）名录中随机抽取。 3年内已接受随机抽查、无违法违规行为的，不列入随机抽查范围。 - 对随机抽查不合格的机构加大抽查频次。	现场、书面、网络检查相结合

国家密码管理局商用密码随机抽查事项清单（2024年版）

商用密码产品检测随机抽查

商用密码应用安全性评估随机抽查

商用密码应用随机抽查

电子认证服务使用密码随机抽查

电子政务电子认证服务随机抽查

03

序号	抽查类别	抽查事项	抽查内容	抽查依据	抽查主体	抽查对象	抽查比例和频次	抽查方式
3	商用密码应用	商用密码应用随机抽查	使用商用密码技术、产品和服务的合规性、正确性、有效性	· 《中华人民共和国密码法》第二十七条、第三十七条 · 《商用密码管理条例》（国务院令760号）第三十八条、第三十九条、第四十一条、第六十条、第六十二条、第六十四条 · 《商用密码应用安全性评估管理办法》（国家密码管理局令3号）第六条、第七条、第八条、第九条、第十条、第十一条、第十二条、第十三条、第十四条、第十五条、第十七条、第十八条	密码管理部门	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安全与信息系统运营者	· 从法律、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安全与信息系统运营者中随机抽取。 · 3年内已接受随机抽查、无违法违规行为的，不列入随机抽查范围。 · 对随机抽查不合格的运营者加大抽查频次。	现场、书面、网络检查相结合

国家密码管理局商用密码随机抽查事项清单（2024年版）

商用密码产品检测随机抽查

商用密码应用安全性评估随机抽查

商用密码应用随机抽

电子认证服务使用密码随机抽查

电子政务电子认证服务随机抽查

04

序号	抽查类别	抽查事项	抽查内容	抽查依据	抽查主体	抽查对象	抽查比例和频次	抽查方式
4	电子认证服务使用密码	电子认证服务使用密码随机抽查	符合许可条件和要求、遵守电子认证服务使用密码相关法律法规和技术规范、规则等情况	《中华人民共和国电子签名法》第十七条 《商用密码管理条例》（国务院令第760号）第二十二条、第二十三条、第五十四条 《电子认证服务密码管理办法》（国家密码管理局公告第17号公布，国家密码管理局公告第32号修正）第三条、第五条、第六条、第七条、第十一条、第十二条、第十三条、第十四条、第十五条、第十六条	密码管理部门	电子认证服务使用密码许可单位	- 从电子认证服务使用密码许可单位名录中随机抽取。 3年内已接受随机抽查、无违法违规行为的，不列入随机抽查范围。 - 对随机抽查不合格的单位加大抽查频次。	现场、书面、网络检查相结合

国家密码管理局商用密码随机抽查事项清单（2024年版）

- 商用密码产品检测随机抽查
- 商用密码应用安全性评估随机抽查
- 商用密码应用随机抽
- 电子认证服务使用密码随机抽查
- 电子政务电子认证服务随机抽查05

序号	抽查类别	抽查事项	抽查内容	抽查依据	抽查主体	抽查对象	抽查比例和频次	抽查方式
5	电子政务电子认证服务	电子政务电子认证服务随机抽查	符合资质认定条件和要求、遵守从业规范、开展电子政务电子认证服务活动等情 况	《中华人民共和国密码法》第二十九条、第三十九条 《商用密码管理条例》（国务院令第760号）第二十四条、第二十五条、第二十八条、第四十七条、第五十五条	密码管理部门	电子政务电子认证服务机构	- 从电子政务电子认证服务机构名录中随机抽取。 3年内已接受随机抽查、无违法违规行为的，不列入随机抽查范围。 - 对随机抽查不合格的机构加大抽查频次。	现场、书面、网络检查相结合

1. 《国家密码管理局商用密码随机抽查事项清单（2024年版）》

2. 抽查依据中涉及的相关法规解读

01 《密码法》

02 《商用密码管理条例》

03 《商用密码检测机构管理办法》

04 《商用密码应用安全性评估管理办法》

3. 炼石免改造数据安全与密码应用实践



第十三届全国人民代表大会常务委员会第十四次会议通过

《中华人民共和国密码法》

（中华人民共和国主席令第三十五号）

2020年1月1日起施行

密码法是我国密码领域的第一部法律



2019年10月26日,十三届全国人大常委会第十四次会议审议通过《中华人民共和国密码法》,自2020年1月1日起施行。

密码法作为我国密码领域的第一部法律,是总体国家安全观框架下,国家安全法律体系的重要组成部分,其颁布实施将极大提升密码工作的科学化、规范化、法治化水平,有力促进密码技术进步、产业发展和规范应用,切实维护国家安全、社会公共利益以及公民、法人和其他组织的合法权益,同时也将为密码部门提高“三服务”能力提供坚实的法治保障。



《密码法》总结构

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

15. 安全保密管理

18. 工作机构和人员管理

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

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

《密码法》内容概要

1

总则

- 规定本法的立法目的，给出密码定义，明确密码工作的基本原则领导和管理体制，明确国家、省、市、县四级密码工作管理体制，提出密码分类管理，以及密码发展促进和保障措施。

2

核心密码、普通密码

- 规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施，包括：安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制、人员管理机制、监督和安全审查制度。

3

商用密码

- 规定了商用密码市场体系、商用密码标准化制度、检测认证制度、网络关键设备和网络安全专用产品目录等市场准入管理制度、关键信息基础设施商密使用要求及密评要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度、商业秘密和个人隐私保护要求。

4

法律责任

- 规定了存在的违法行为、商用密码检测/认证机构、关键信息基础设施的运营者、密码管理部门和有关部门/单位的工作人员等违反本法相关规定应当承担的相应的法律后果。

5

附则

- 规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的施行日期。

立法背景和必要性

密码是国家重要战略资源，密码工作也是党和国家的一项特殊重要工作，直接关系到国家政治安全、经济安全、国防安全和信息安全。在我国革命、建设、改革各个历史时期，都发挥了不可替代的重要作用。在密码法出台前，我国密码领域核心密码和普通密码都是通过政策性文件来管理，商用密码则是通过《商用密码管理条例》这一部行政法规来管理。无论是在立法位阶上，还是在法律效力上，均已不能适应新时代密码事业发展的需要，亟须制定一部综合性、基础性法律，把密码工作各领域、各环节、各要素纳入法治轨道。



推进密码立法

核心密码和普通密码维护国家安全方面的基本制度，密码管理部门和密码工作机构及其工作人员开展核心密码和普通密码工作的保障措施等，需要通过国家立法予以明确，进一步提升法治化保障水平。



提升密码法制化

近年来密码在维护国家安全、促进经济社会发展、保护人民群众利益方面发挥越来越重要的作用，国家对重要领域商用密码的应用、基础支撑能力的提升以及安全性评估、审查制度等不断提出明确要求，需要及时上升为法律规范。



满足新时代新要求

传统对商用密码实行全环节许可管理的手段，已不适应职能转变和“放管服”改革要求，急需在立法层面重塑现行商用密码管理制度。

重要意义

密码法是构建国家安全法律制度体系的重要举措

党的十八届四中全会提出，贯彻落实总体国家安全观，加快国家安全法治建设，构建国家安全法律制度体系。

密码工作直接关系国家政治安全、经济安全、国防安全和信息化安全。党中央高度重视密码立法工作，将密码法作为国家安全法律制度体系的重要组成部分，强调要在国家安全法治建设的大盘子中研究制定密码法，把党对密码工作的最新要求通过法定程序转化为国家意志。

把密码应用和管理的基本制度及时上升为法律规范，填补了我国密码领域长期存在的法律空白。推动构建以密码技术为核心、多种技术交叉融合的网络空间新安全体制，对于加快密码法治建设，理顺国家安全领域相关法律法规关系，完善国家安全法律制度体系具有重要意义。

密码法是维护国家网络空间主权安全的重要举措

密码是目前世界上公认的，保障网络与信息安全最有效、最可靠、最经济的关键核心技术。在信息化高度发展的今天，密码的应用已经渗透到社会生产生活各个方面，从涉及政权安全的保密通信、军事指挥，到涉及国民经济的金融交易、防伪税控，再到涉及公民权益的电子支付、网上办事等等，密码都在背后发挥着基础支撑作用。

制定和实施密码法，就是要把密码应用和管理的基本制度及时上升为法律规范，推动构建以密码技术为核心、多种技术交叉融合的网络空间新安全体制，努力做到党和国家战略推进到哪里，密码就保障到哪里。

密码法是推动密码事业高质量发展的重要举措

党的十八大以来，在以习近平同志为核心的党中央坚强领导下，在中央密码工作领导小组领导指挥下，密码事业取得历史性成就、实现历史性变革。

制定和实施密码法，就是要适应新的形势发展需要，推进密码领域职能转变和“放管服”改革，建立健全密码法治实施、监督、保障体系，规范密码产业秩序，提升密码自主创新水平和供给能力，为密码事业又好又快发展提供制度保障。

立法思路

密码法立法过程中，重点把握以下三个原则

1

明确对核心密码、普通密码与 商用密码实行分类管理的原则

在核心密码、普通密码方面，深入贯彻总体国家安全观，将现行有效的基本制度、特殊管理政策及保障措施法治化；在商用密码方面，充分体现职能转变和“放管服”改革要求，明确公民、法人和其他组织均可依法使用。

2

注重把握职能转变和“放管服” 要求与保障国家安全的平衡

在明确鼓励商用密码产业发展、突出标准引领作用的基础上，对涉及国家安全、国计民生、社会公共利益，列入网络关键设备和网络安全专用产品目录的产品，以及关键信息基础设施的运营者采购等部分，规定了适度的管制措施。

3

注意处理好密码法与网络安全法、 保守国家秘密法等有关法律的关系

在商用密码管理和相应法律责任设定方面，与网络安全法的有关制度，如强制检测认证、安全性评估、国家安全审查等作了衔接；同时，鉴于核心密码、普通密码属于国家秘密，在核心密码、普通密码的管理方面与保守国家秘密法作了衔接。

主要内容-什么是密码？

密码法共五章四十四条，重点规范了以下内容

明确密码定义

密码法中的密码, 第二条规定“是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”。

密码是保障网络与信息安全的核心技术和基础支撑, 是解决网络与信息安全问题最有效、最可靠、最经济的手段; 它就像网络空间的DNA, 是构筑网络信息系统免疫体系和网络信任体系的基石, 是保护党和国家根本利益的战略性资源, 是国之重器。

密码的种类及其适用范围

第六条至第八条规定, 明确了密码的种类及其适用范围。按照保护信息的种类不同, 将密码分为:

核心密码

普通密码

商用密码

规定核心: 密码用于保护国家绝密级、机密级、秘密级信息;

普通密码: 用于保护国家机密级、秘密级信息;

商用密码: 用于保护不属于国家秘密的信息。

对密码实行分类管理 是党中央确定的密码管理根本原则, 是保障密码安全的基本策略, 也是长期以来密码工作经验的科学总结。

主要内容-谁来管密码？

确立密码工作领导体制

第四条规定，要坚持党管密码根本原则，依法确立密码工作领导体制。

明确中央密码工作领导机构，即中央密码工作领导小组（国家密码管理委员会），对全国密码工作实行统一领导；要把中央确定的领导管理体制，通过法律形式固定下来，变成国家意志，为密码工作沿着正确方向发展提供根本保证。

中央密码工作领导小组负责制定国家密码重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。

四级密码工作管理体制

第五条规定，确立了国家、省、市、县四级密码工作管理体制。

国家密码管理部门：即国家密码管理局，负责管理全国的密码工作；

县级以上地方各级密码管理部门：即省、市、县级密码管理局，负责管理本行政区域的密码工作；

国家机关和涉及密码工作的单位：在其职责范围内负责本机关、本单位或者本系统的密码工作。

主要内容-怎么管密码？

核心密码、普通密码的主要管理制度

第二章(第十三条至第二十条)规定了核心密码、普通密码的主要管理制度。密码法明确规定：**密码管理部门依法对核心密码、普通密码实行严格统一管理，并规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。**

核心密码、普通密码本身就是国家秘密，一旦泄密，将危害国家安全和利益。因此，有必要对核心密码、普通密码的科研、生产、服务、检测、装备、使用和销毁等各个环节实行严格统一管理，确保核心密码、普通密码的安全。

商用密码的主要管理制度

第三章(第二十一条至第三十一条)规定了商用密码的主要管理制度。密码法明确规定，**国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。**

商用密码广泛应用于国民经济发展和生产生活的方方面面，涵盖金融和通信、公安、税务、社保、交通、卫生健康、能源、电子政务等重要领域，积极服务“互联网+”行动计划、智慧城市和大数据战略，在维护国家安全、促进经济社会发展以及保护公民、法人和其他组织合法权益等方面发挥着重要作用。

坚决贯彻落实“放管服”改革要求

充分体现非歧视和公平竞争原则，进一步削减行政许可数量，放宽市场准入，更好地激发市场活力和社会创造力。

严格管理调整为重点把控

由商用密码管理条例规定的全环节严格管理调整为重点把控产品销售、服务提供、使用、进出口等关键环节，管理方式上由重事前审批转为重事中事后监管，重视发挥标准化和检测认证的支撑作用。

行政许可和管制措施

对于关系国家安全和社会公共利益，又难以通过市场机制或者事中事后监管方式进行有效监管的少数事项，规定了必要的行政许可和管制措施。按照上述立法思路，密码法规定了商用密码的主要管理制度，包括商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码安全

主要内容-怎么用密码？

核心密码、普通密码的使用要求

第十四条要求：在有线、无线通信中传递的国家秘密信息，以及存储、处理国家秘密信息的信息系统，应当依法使用核心密码、普通密码进行**加密保护、安全认证**。

关键信息基础设施密码使用要求

第二十七条要求关键信息基础设施必须依法使用商用密码进行保护，并开展商用密码应用安全性评估；
要求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办会同国家密码管理局等有关部门组织的国家安全审查。
党政机关存在大量的涉密信息、信息系统和关键信息基础设施，都必须依法使用密码进行保护。

商用密码的使用要求

第八条规定公民、法人和其他组织可以依法使用商用密码保护网络与信息安全，对一般用户使用商用密码没有提出强制性要求。

密码两用物项相关规定

由于密码属于两用物项，第十二条还明确规定，任何组织或者个人：

- 不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统
- 不得利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犯罪活动

主要内容-怎样保障和促进密码的发展？

法案总则对核心密码、普通密码和商用密码在发展促进和保障措施方面的共性内容作了规定

鼓励和支持密码科学技术研究、交流

第九条规定国家鼓励和支持密码科学技术研究、交流，依法保护密码知识产权，促进密码科学技术进步和创新，建立密码工作表彰奖励制度。

加强密码安全教育

第十条规定，国家采取多种形式加强密码安全教育，将密码安全教育纳入国民教育体系和公务员教育培训体系，增强公民、法人和其他组织的密码安全意识。

密码工作纳入本级国民经济和社会发展规划

第十一条，规定县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级预算。

国务院第4次常务会议修订通过

《商用密码管理条例》

（中华人民共和国国务院令 第760号）

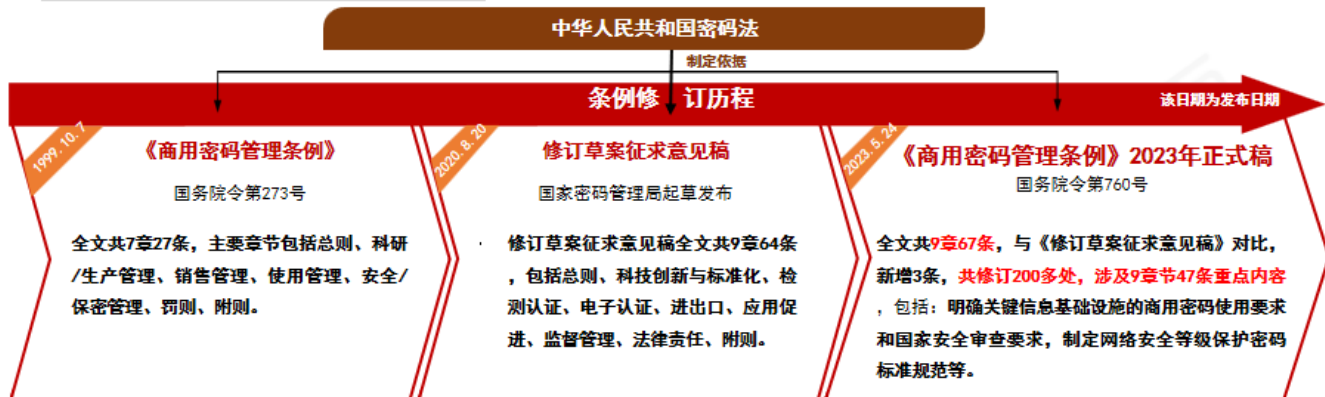
2023年7月1日起施行

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》正式发布，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使用规范；
- 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

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. 高密检测认证体系 | 13. 高密检测机构资质认定 | 14. 检测资质取得条件 |
| 15. 检测机构资质申请流程 | 16. 高密检测实施要求 | 17. 高密认证制度 |
| 18. 高密认证机构能力要求 | 19. 高密认证实施要求 | 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. 未经认定的高密检测或电子认证服务处罚 | 51. 高密检测机构违法行为处罚 | 52. 高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. 进出口高密的处罚 | 59. 窃取加密信息、非法入侵密码系统等违法活动的处罚 | 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. 阻挠高密监督管理的处罚 | 64. 国家机关违法行为的处罚 | 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高密
36. 支持网络产品/服务使用高密应用
37. 应用促进协调机制
38. 关基密评要求
39. 关基高密产品/服务使用要求
40. 关基运营者采购高密产品和服务的安全审查机制
41. 网络运营者等保遵循/制定网络安全等级保护密码标准规范
42. 密评、关基检测、等保加强衔接避免重复评估

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、监管、惩戒、修复机制
47. 保密义务
48. 高密监督管理
49. 举报机制

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。

3. 检测认证

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

- 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、认证机构检测认证合格后，方可销售或者提供。

7. 监督管理

关键领域商用密码**服务** 实行**强制性**认证

- 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。

8. 法律责任

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

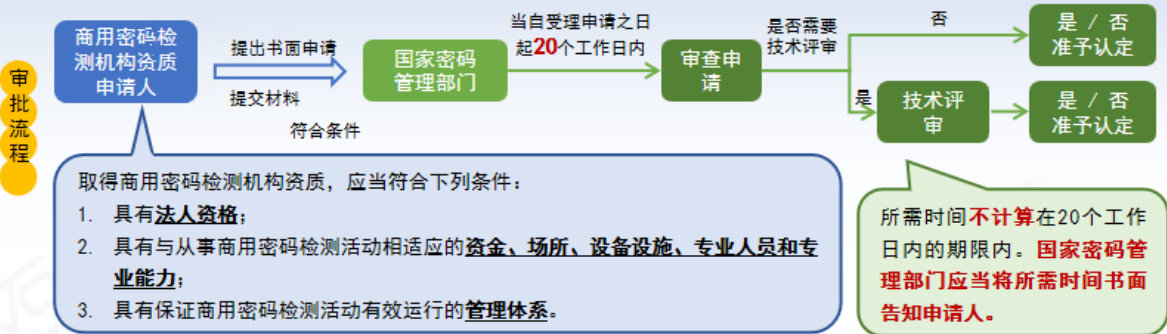
6. 应用促进

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

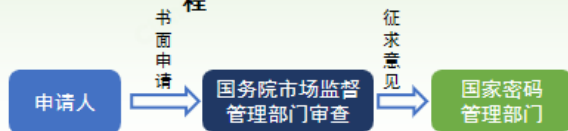
8. 法律责任

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

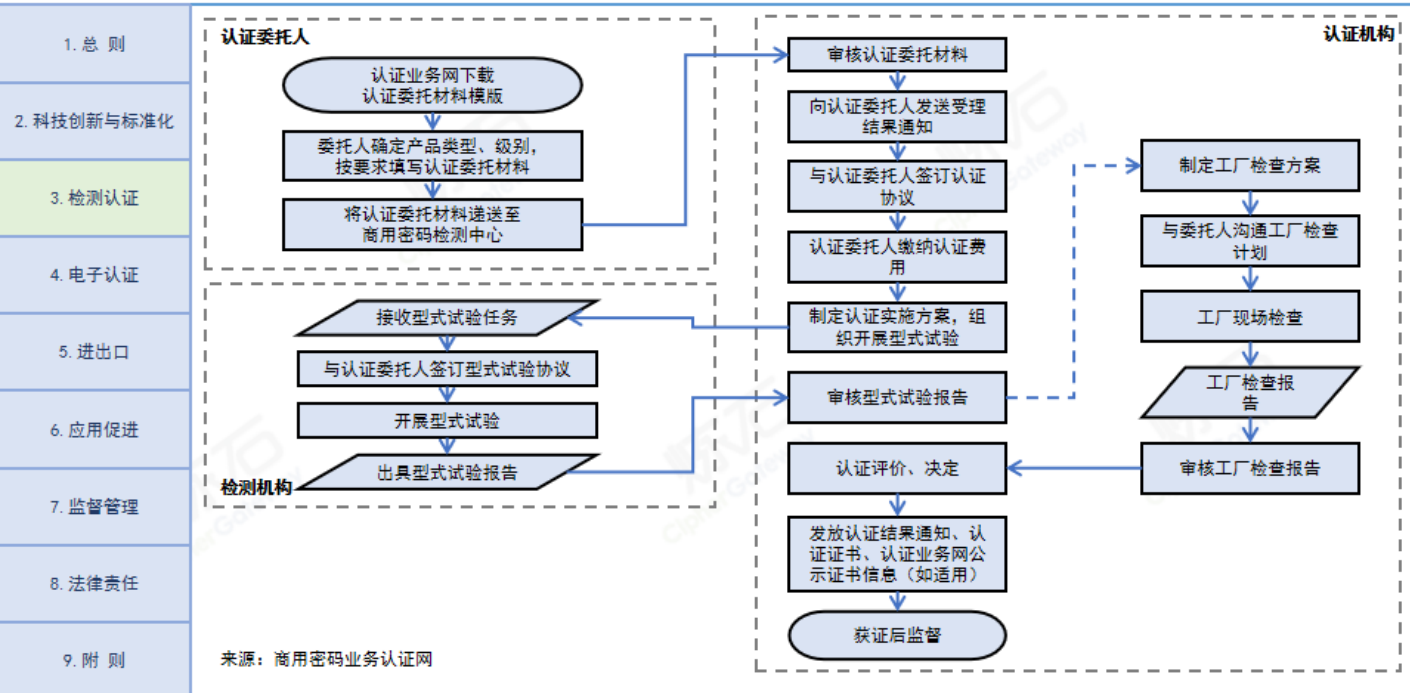


申请人除应当符合法律、行政法规和国家有关规定要求的认证机构基本条件外，还应当具备与从事商用密码认证活动相适应的商用密码检测、检查、标准研制与验证等专业能力。

国务院市场监督管理部门在审查商用密码认证机构资质申请时，应当征求国家密码管理部门的意见。

- 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

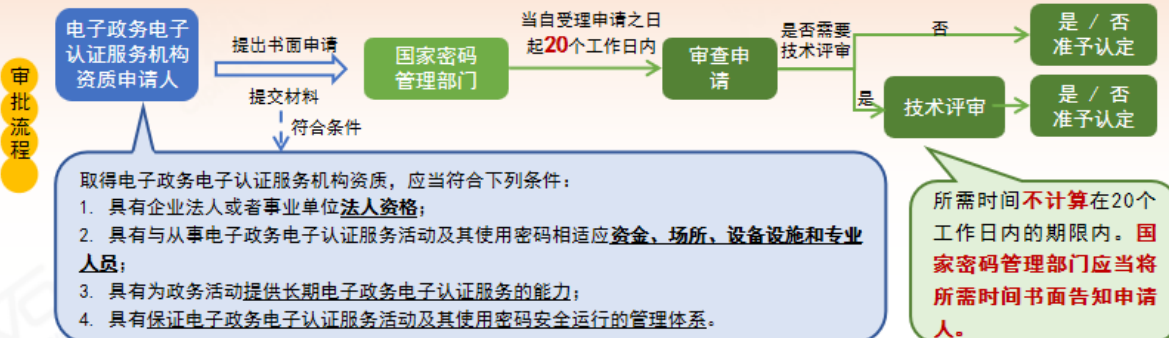
6. 应用促进

7. 监督管理

8. 法律责任

9. 附 则

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



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、直辖市密码管理部门报送服务实施情况**

国家建立统一的电子认证信任机制

1. 总 则	
2. 科技创新与标准化	国家 建立<u>统一</u>的电子认证信任机制
3. 检测认证	
4. 电子认证	国家密码管理部门 - 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	
6. 应用促进	密码管理部门会同有关部门 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	
8. 法律责任	电子政务电子认证服务机构 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	

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

	进出口许可申请	进出口许可证申请	进出口许可证交验	进出口放行
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				

```

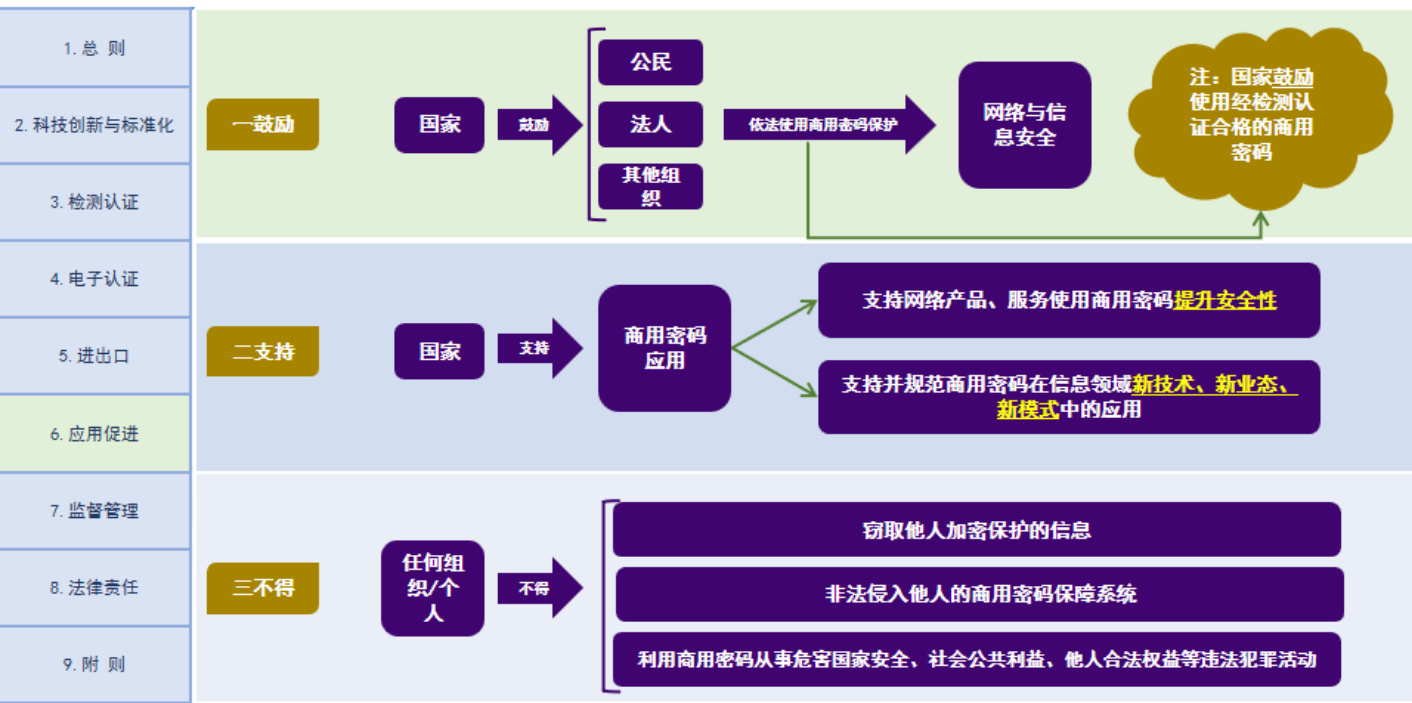
graph TD
    A[相关企业/组织  
(进出口经营者)] -- "提出书面申请,  
提交证明材料" --> B[国务院商务主管部门会同国家密码管理部门依法对申请进行审查]
    B -- "未许可" --> C{是否准予许可}
    C -- "许可" --> D{是否属于进口许可或出口管制清单}
    D -- "是" --> E[向国务院商务主管部门申请领取进出口许可证]
    D -- "否" --> F[海关确认是否属于进口许可或出口管制范围]
    F -- "海关有证据表明进出口产品可能属于商用密码进口许可清单或者出口管制清单范围的,应当向进出口经营者提出质疑" --> G[海关可以向国务院商务主管部门提出组织鉴别]
    G --> H{鉴别结论}
    H -- "不属于" --> I[办理报关手续]
    H -- "属于进口许可或出口管制范围" --> E
    I --> J[海关放行]
    K[在鉴别或者质疑期间, 海关对进出口产品不予放行] -.-> L[海关放行]
    
    Note1["适用范围: 商用密码的过境、转运、通运、再出口, 在境外与综合保税区等海关特殊监管区域之间进出, 或者在境外与出口监管仓库、保税物流中心(含保税物流园区)之间进出"]
    Note2["书面材料: (一) 申请人的法定代表人、主要经营管理人员以及经办人的身份证明;(二) 合同或者协议的副本;(三) 商用密码的技术说明;(四) 最终用户和最终用途证明;(五) 国务院商务主管部门规定提交的其他文件。"]
    
```

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》由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并公布。**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

统筹
指导

各司
其职

加强
管理

国家

建立

商用密码应用促进
协调机制

目的

加强对商用密码应用的
统筹指导

国家机关和涉及
商用密码工作的
单位

负责

各自职责范围内，负责本
机关、本单位或者本系统
的商用密码应用和安全保
障工作

密码管理部门
会同有关部门

加强

商用密码
应用信息
收集、风
险评估、
信息通报
和重大事
项会商

与网络安
全监测预
警和信息
通报的衔
接

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	<u>使用商用密码进行保护</u>	其运营者应当使用商用密码进行保护， <u>制定商用密码应用方案</u> ，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		<u>制定商用密码应用方案</u>	
		<u>同步规划、同步建设、同步运行商用密码保障系统</u>	网络运营者应当 <u>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</u> 。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。
3. 检测认证		<u>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</u>	
4. 电子认证		<u>运行后每年至少进行一次评估</u>	
5. 进出口		<u>商用密码技术应当通过国家密码管理部门审查鉴定</u>	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， <u>运行后每年至少进行一次评估</u> ，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。
6. 应用促进			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 <u>商用密码技术应当通过国家密码管理部门审查鉴定</u> 。
7. 监督管理			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， <u>避免重复评估、测评</u> 。
8. 法律责任		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， <u>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。</u>	
9. 附 则			

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

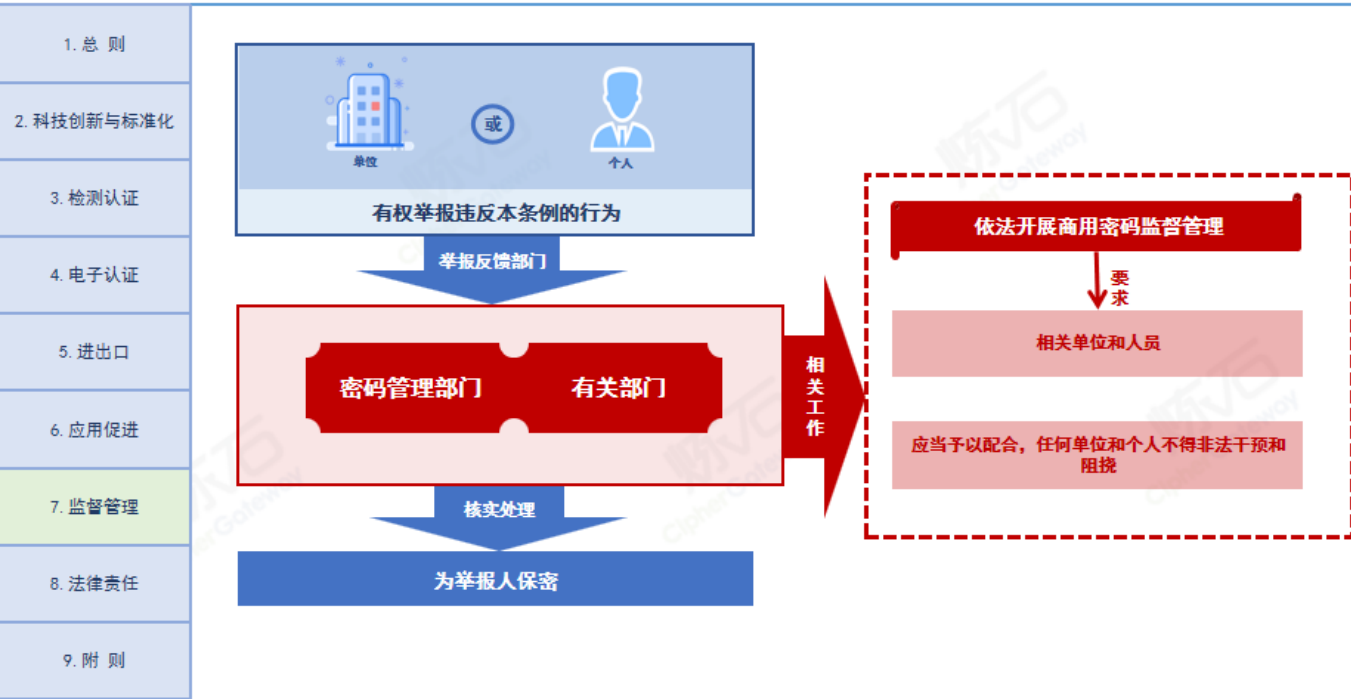
7. 监督管理

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



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	企业或机构		
2. 科技创新与标准化		违反本条例规定， 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	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， 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	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； 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 ；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			
6. 应用促进		违反本条例规定， 未经批准从事商用密码认证活动的	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， 构成犯罪	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： (一) 超出批准范围； (二) 存在影响检测独立、公正、诚信的行为； (三) 出具的检测数据、结果虚假或者失实； (四) 拒不报送或者不如实报送实施情况； <u>(五) 未履行保密义务；</u> (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。	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； <u>情节严重的，依法吊销商用密码检测机构资质。</u>
2. 科技创新与标准化			
3. 检测认证			
4. 电子认证			
5. 进出口	商用密码认证机构	开展商用密码认证，有下列情形之一的 (一) 超出批准范围； (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； <u>(五) 未履行保密义务；</u> (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。	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； <u>情节严重的，依法吊销商用密码认证机构资质</u>
6. 应用促进			
7. 监督管理			
8. 法律责任	电子认证服务机构	<u>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</u>	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； <u>情节严重的，依法吊销电子认证服务使用密码的证明文件。</u>
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	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) 未履行保密义务； (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； 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。
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	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		
6. 应用促进		违反本条例第三十条规定，未由依法设立的电子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	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， 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。
8. 法律责任		违反本条例第四十条规定， 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	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10万元以下罚款。
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

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	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。
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5万元以下罚款。</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

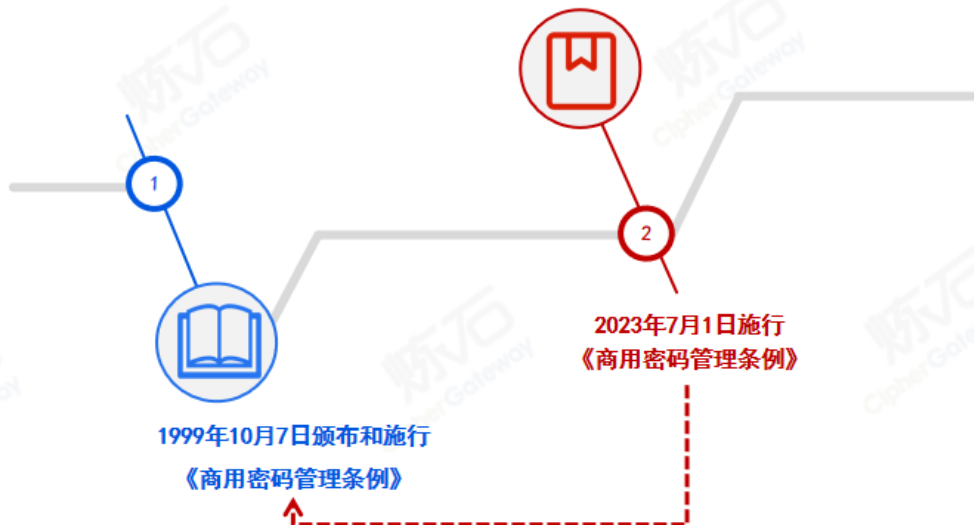
5. 进出口

6. 应用促进

7. 监督管理

8. 法律责任

9. 附 则



国家密码管理局

《商用密码检测机构管理办法》

（国家密码管理局令第2号）

2023年11月1日起施行

加强密评机构管理，规范商用密码检测活动

**国家密码管理局**
WWW.SCA.GOV.CN

请输入关键词

热门搜索: 商用密码 电子认证 电子政务

首页 | 机构概况 | 新闻动态 | 信息公开 | 在线服务 | 互动交流 | 专题专栏

首页 > 信息公开 > 政策法规 > 部门规章

商用密码检测机构管理办法 (国家密码管理局令第2号)

发布日期: 2023-10-07 来源:

【字体: 大 中 小】  打印

国家密码管理局令

第 2 号

《商用密码检测机构管理办法》已经2023年9月11日国家密码管理局局务会议审议通过，现予公布，自2023年11月1日起施行。

局 长 刘东方
2023年9月26日

商用密码检测机构管理办法

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。

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。

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

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。

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

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。

迫切需求

是规范商用密码检测机构管理的迫切需要

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	坚持保障安全和创新发展的统一
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，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、做大做强的</u> 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

规定了本办法的施行时间。

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

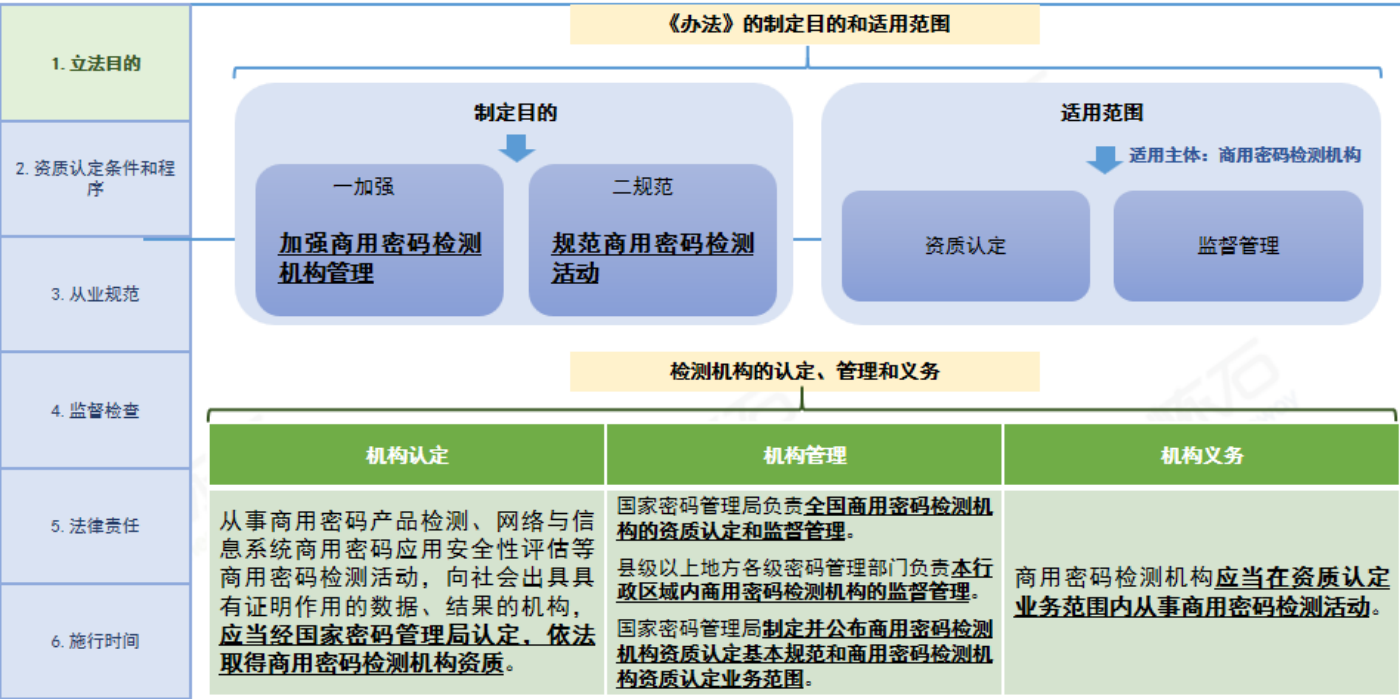
27. 监督管理信息公示

28. 监管人员违规处罚

六、施行时间

29. 施行日期

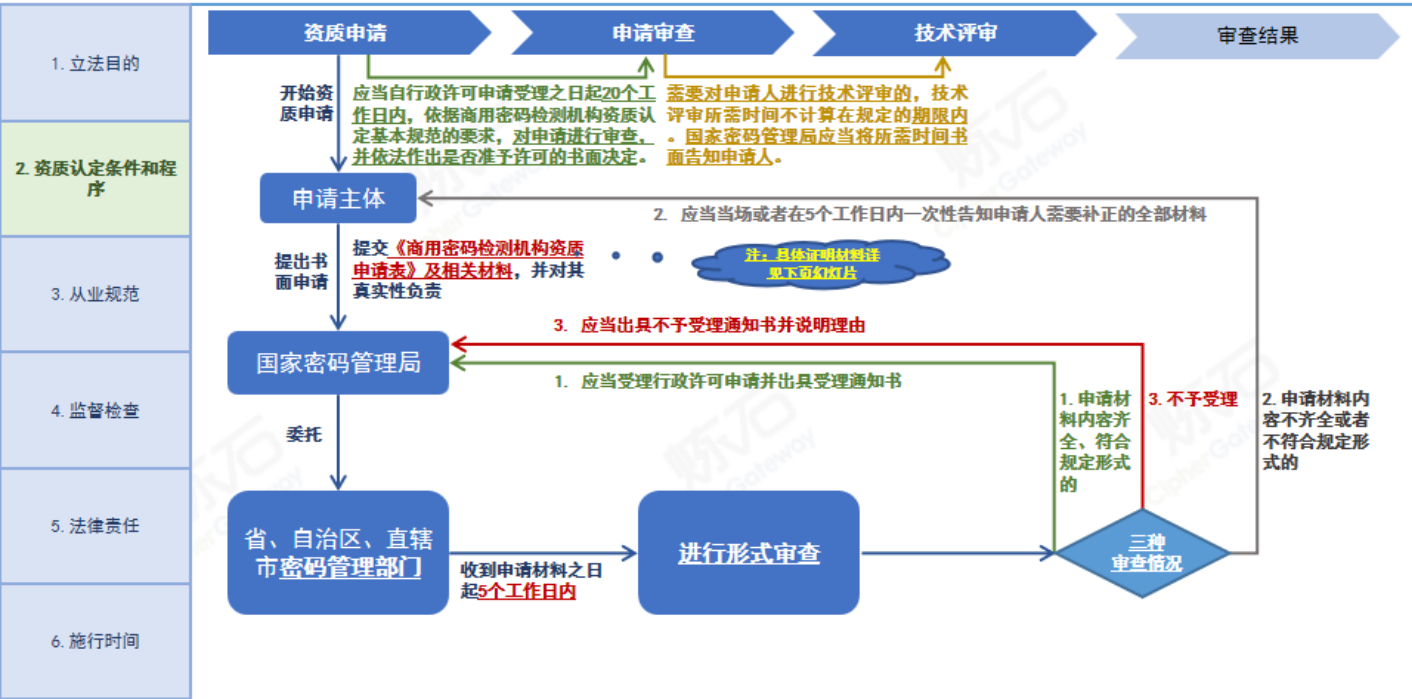
办法制定将加强机构管理以及规范商密检测活动



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>
	(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>
3. 从业规范	(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法规的规定</u>	

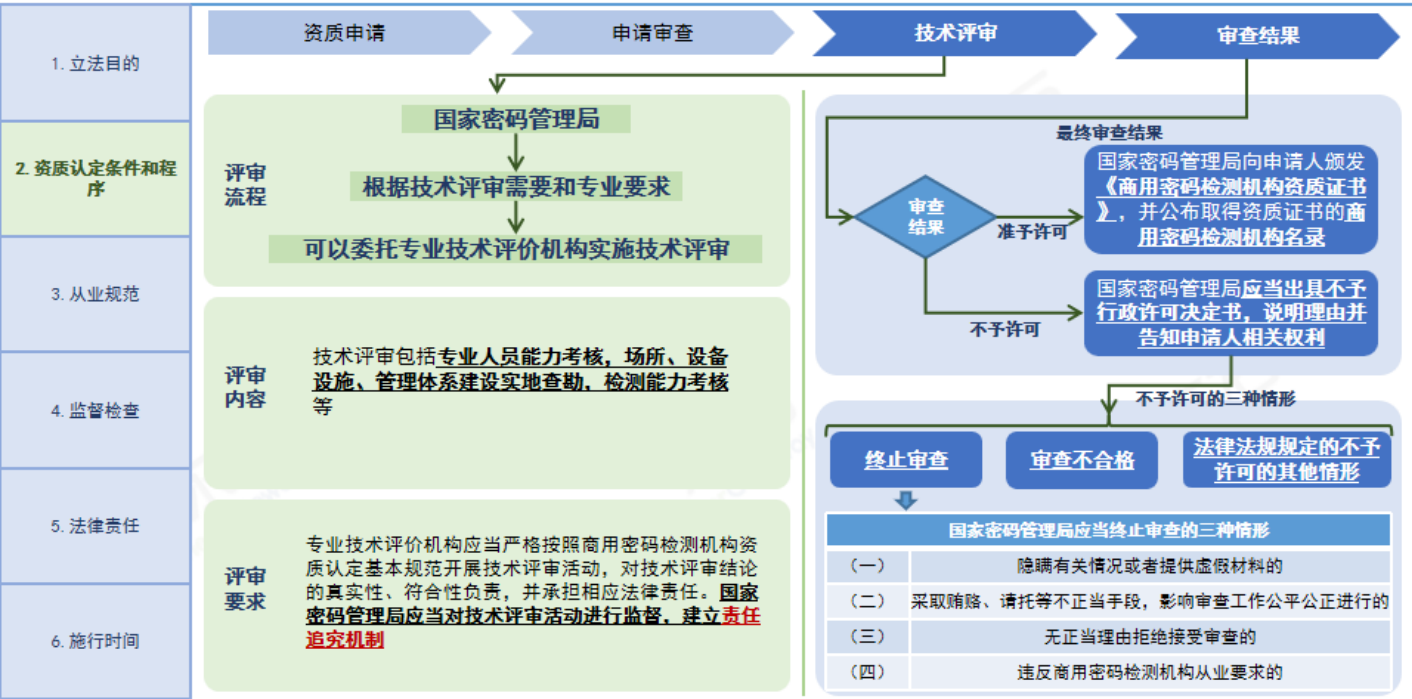
申请商用密码检测机构资质应当向国家密码管理局提出书面申请



资质申请时需要提交的相关材料列表

1. 立法目的	资质申请 申请审查 技术评审 审查结果 ↓ 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			
3. 从业规范	(一)	法人资格证书		
4. 监督检查	(二)	资本结构和股权情况		
	(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		
5. 法律责任	(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		
6. 施行时间	(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		
	(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		

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



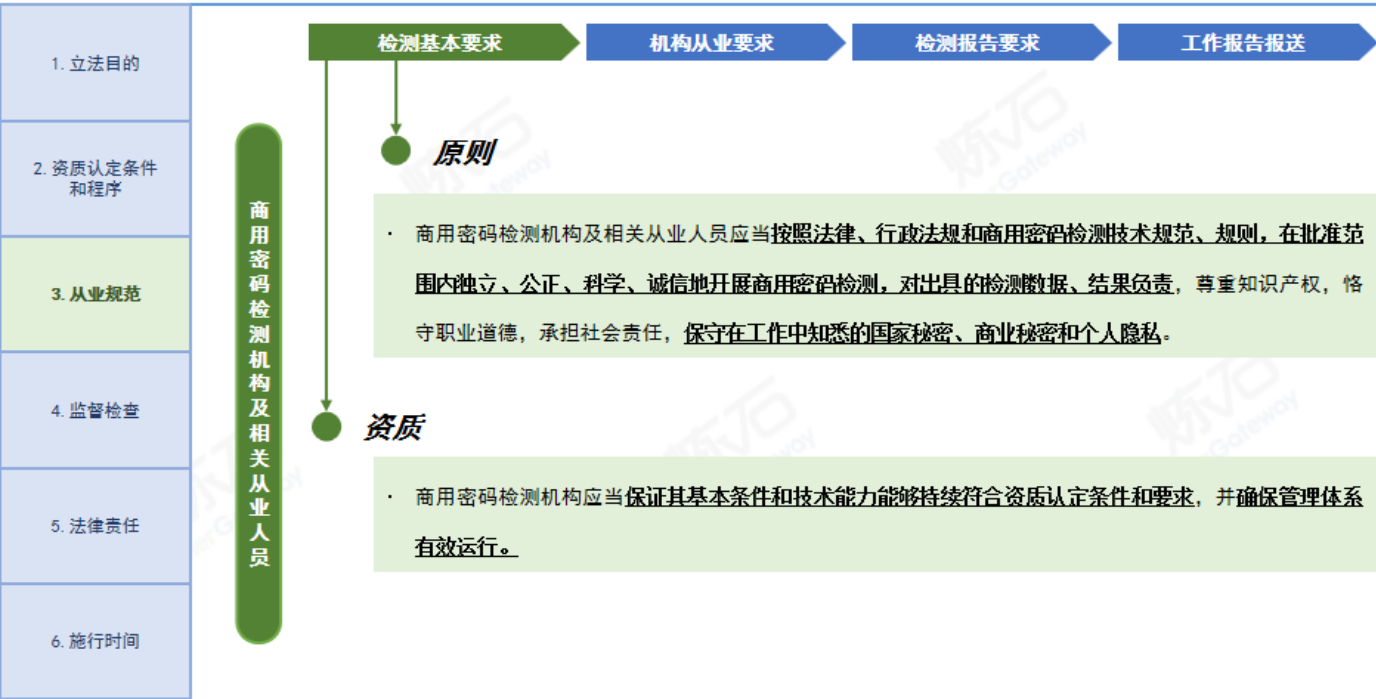
有效期届满需要延续的应当在有效期届满3个月前提出书面申请

1. 立法目的	证书内容		证书有效期		禁止情形	
2. 资质认定条件和程序	证书内容列表		有效期5年，有效期届满需要重新申请，具体流程如下： 申请人 有效期届满需要延续的，应当在有效期届满3个月前向国家密码管理局提出书面申请 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 开展审查 在《商用密码检测机构资质证书》有效期届满前作出是否准予延续的决定		证书禁止情形	
3. 从业规范	(一)	获证机构名称			(一)	转让
4. 监督检查	(二)	统一社会信用代码			(二)	出租
5. 法律责任	(三)	注册地址			(三)	出借
6. 施行时间	(四)	证书编号			(四)	伪造
	(五)	有效期限			(五)	变造
	(六)	资质认定业务范围			(六)	冒用
	(七)	发证机关			(七)	租借
	(八)	发证日期				

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：	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：
3. 从业规范	(一) 机构名称、注册地址、法人性质发生变更的	(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
4. 监督检查	(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	(二) 申请注销商用密码检测机构资质的
5. 法律责任	(三) 资质认定业务范围发生变更的	(三) 被依法撤销、吊销商用密码检测机构资质的
6. 施行时间	(四) 依法需要办理变更的其他事项	(四) 依法终止的
	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。	(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

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

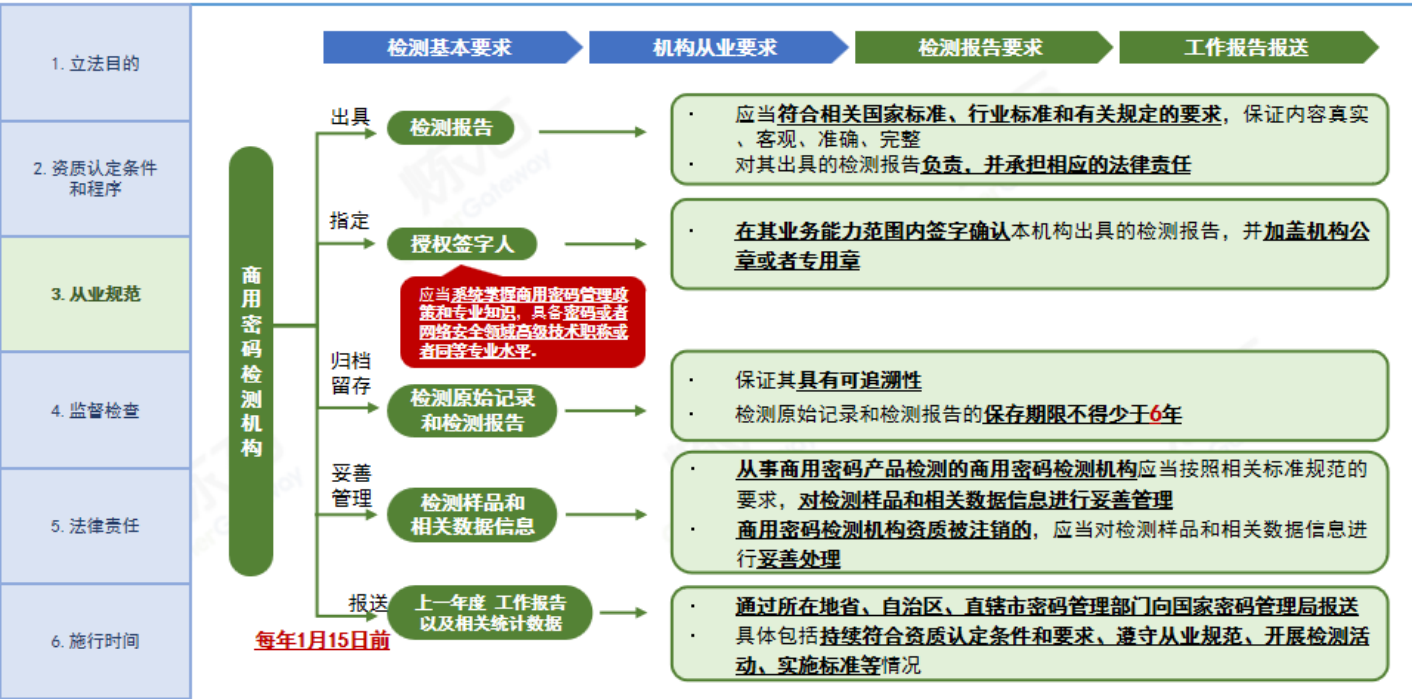
	检测基本要求	机构从业要求	检测报告要求	工作报告报送
1. 立法目的				
2. 资质认定条件和程序				
3. 从业规范	商用密码检测机构  安全保密教育和业务培训 · 加强对本机构人员的监督管理，经常性组织开展安全保密教育和业务培训；本机构从事检测活动的专业人员每年接受商用密码教育培训的时长不得少于40学时，相关情况应当记录留存；  不得从事影响检测公平公正活动 · 本机构及关联方不得从事商用密码产品生产、销售（检测工具除外），信息系统或者商用密码保障系统集成、运营，电子认证服务，电子政务电子认证服务，或者其他可能影响商用密码检测公平公正性的活动；	 不得恶意竞争 · 不得同时聘用正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；	
4. 监督检查				
5. 法律责任	 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。
6. 施行时间				



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；**

明确检测报告要求及工作报告报送规范



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

禁止虚报/
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



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 欺骗、贿赂等不正当手段 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 隐瞒有关情况或者提供虚假材料 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；	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
4. 监督检查	· 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；		· 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
5. 法律责任	· 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； · 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；		· 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
6. 施行时间	· 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； · 泄露在工作中知悉的商业秘密、个人隐私的。	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

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： · 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管理检测样品和相关数据信息的。	密码管理部门	· 责令改正
2. 资质认定条件和程序			· 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
3. 从业规范		县级以上地方各级密码管理部门	· 依法公开监督检查结果，将商用密码检测机构受到的行政处罚等信息纳入国家企业信用信息公示系统等平台
4. 监督检查			· 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
5. 法律责任	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	—	· 依法给予处分
6. 施行时间			

***本办法自2023年11月1日起施行。**

国家密码管理局

《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）

2023年11月1日起施行

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



《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、遵循同一套活动”,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**。

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。

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。

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，对网络与信息系统中使用商用密码技术、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

1. 总体要求

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

“重要网络与信息系统”如何界定？

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系统包括：基础信息网络、涉及国计民生和基础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。”

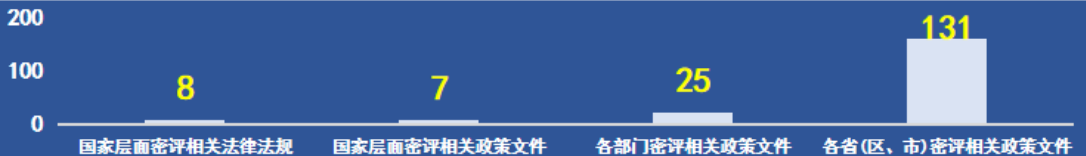
目前对“重要网络与信息系统”界定，依据是“法律、行政法规和国家有关规定”，可参考本文P10-23的政策清单（附录1-4）

3. 实施规范

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：

4. 监督检查及法律责任

5. 其他事项



附录1 国家层面密码应用及密评相关法律法规

发文/起草单位	发布/施行时间 (注:已发布法律法规为“施行时间”,其他为“发布时间”)	政策文件	相关内容
第十三届全国人民代表大会常委会第十四次会议通过	2020年1月1日	《密码法》 (中华人民共和国主席令第三十五号)	第二十七条: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关键信息基础设施,其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、网络安全等级测评制度相衔接,避免重复评估、测评。 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,应当按照《中华人民共和国网络安全法》的规定,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。
第十二届全国人民代表大会常委会第二十四次会议通过	2017年6月1日	《网络安全法》 (中华人民共和国主席令第五十三号)	第十条:建设、运营网络或者通过网络提供服务,应当依照法律、行政法规的规定和国家标准的强制性要求,采取技术措施和其他必要措施,保障网络安全、稳定运行,有效应对网络安全事件,防范网络违法犯罪活动,维护网络数据的完整性、保密性和可用性。 第二十一条:采取数据分类、重要数据备份和加密等措施。
第十三届全国人民代表大会常委会第二十九次会议通过	2021年9月1日	《数据安全法》 (中华人民共和国主席令第八十四号)	第二十七条:开展数据处理活动应当依照法律、法规的规定,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。利用互联网等信息网络开展数据处理活动,应当在网络安全等级保护制度的基础上,履行上述数据安全保护义务。
第十三届全国人民代表大会常委会第三十次会议通过	2021年11月1日	《个人信息保护法》 (中华人民共和国主席令第九十一号)	第五十一条:个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等,采取下列措施确保个人信息处理活动符合法律、行政法规的规定,并防止未经授权访问以及个人信息泄露、篡改、丢失: (三)采取相应的加密、去标识化等安全技术措施。

发文/起草单位	发布/施行时间 (注:已发布法律法规为“施行时间”,其他为“发布时间”)	政策文件	相关内容
国务院第4次常务会议修订通过	2023年4月14日	《商用密码管理条例》	第三十八条: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。 前款所列关键信息基础设施通过商用密码应用安全性评估后方可投入运行。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。 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、网络安全等级测评应当加强衔接,避免重复评估、测评。
公安部会同相关部门	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。三级以上网络应当采用密码保护,并使用国家密码管理部门认可的密码技术、产品和服务。 三级以上网络运营者应在网络规划、建设和运行阶段,按照密码应用安全性评估管理办法和相关标准,委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后,方可上线运行,并在投入运行后,每年至少组织一次评估。密码应用安全性评估结果应当报送受理备案的公安机关和所在地设区市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》	第五十条:存储、处理涉及国家秘密信息的关键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	《网络数据安全条例(征求意见稿)》	第九条:数据处理者应当采取备份、加密、访问控制等必要措施,保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用,应对数据安全事件,防范针对和利用数据的违法犯罪活动,维护数据的完整性、保密性、可用性。 数据处理者应当使用密码对重要数据和核心数据进行保护。

附录2 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	《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）	第三章“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、保密监测预警和密码应用安全性评估的机制，定期开展网络安全、保密和密码应用检查，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，强化密码应用安全性评估，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、追踪溯源和精准授权能力。
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码应用安全性评估。
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、同步运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靠情况，项目密码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 第 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风险入口。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。

附录3 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18日	《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技术人员，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。
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，其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试点工作的通知》（国密码局〔2022〕454号）	进一步加强对密评试点工作的督促指导，强调重要网络与系统运营者密评主体责任，规范密评试点机构的日常监督，严格密评结果备案材料的形式审查，包括对密评活动真实性、密评实施规范性、密评记录清晰准确性、密评报告完整合规性等运行形式审查，并明确了密评机构、各级密码管理部门违规行为的惩罚措施。
国家能源局	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“电力企业责任义务”第十五条中提出：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安全审查等工作，未达到要求的应当及时进行整改。
国家卫生健康委、国家中医药局、国家疾控局	2022年8月8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”第十五条中提出：各医疗卫生机构应当按照《密码法》等有关法律法规和密码应用相关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。

发文/起草单位	发文时间	政策文件	相关内容
国家邮政局、国家发展改革委员会、交通运输部	2021年12月28日	《“十四五”邮政业发展规划》	第二章“主要任务”第六条“提高行业安全水平”中第十九点提出：加强网络安全。严格落实网络安全工作责任制，完善行业网络安全、数据安全有关标准规范。在网络建设和运营过程中，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、关保、密评等有关要求。加强行业关键信息基础设施保护，组织编制相关规划，强化行业指导和监督。加强行业重要数据和个人信息保护。
民政部	2021年12月23日	《关于印发〈“十四五”民政信息化发展规划〉的通知》（民发〔2021〕104号）	第三章“重点任务”第四条中提出：全面开展国产商用密码应用，构建民政统一的密码应用基础服务平台，提供统一的数据传输、存储加密和身份认证管理等相关服务，提升密码使用和管理水平。
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装备工作的通知》（国密码局〔2021〕392号）	网络与信息系统运营者同步规划、同步建设、同步运行商用密码保障系统，规范开展密评工作，履行备案程序。密码管理机构对密评机构的备案材料进行形式审查，定期收集汇总备案信息，按季度报送国家密码管理局。密评机构按年度统计密评工作情况报送国家密码管理局。
国家密码管理局、中央网信办、国家发展改革委员会、科技部、工业和信息化部、公安部、财政部、国务院国资委、市场监管总局、证监会	2021年11月20日	《促进商用密码产业高质量发展相关文件》	依法督促建设密码保障体系，并强化重要网络与信息系统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	《关于加强车联网网络安全和数据安全工作的通知》（工信部网安〔2021〕134号）	第四章“加强车联网服务平台安全防护”第十条中提出：认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准使用商用密码进行保护，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。
工业和信息化部、中央网信办、科技部、生态环境部、住房和城乡建设部、农业农村部、国家卫生健康委员会、国家能源局	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〕130号）	第二章“重点任务”第四章“支撑体系优化行动”中第十二点提出：加快物联网领域商用密码技术和产品的应用推广，建设面向物联网领域的密码应用检测平台，提升物联网领域商用密码安全性和应用水平。

附录3 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、国家发展改革委、教育部、财政部、住房和城乡建设部、文化和旅游部、国家卫生健康委员会、国家能源局	2021年7月5日	《5G应用“扬帆”行动计划（2021-2023年）》（工信部通信〔2021〕77号）	第四章“提升5G应用支撑能力”第三条“5G应用安全提升行动”中第三十条提出：在5G应用中推广使用商用密码，做好密码应用安全性评估。
交通运输部办公厅	2021年5月27日	《关于印发〈城市轨道交通自动驾驶系统运营技术规范（试行）〉的通知》（交办运〔2021〕27号）	第九章“互联网设备”第9.3条“运营安全”中第9.3.3点提出：互联网设备的密码使用和管理应符合国家网络安全及商用密码管理的法律法规，并保证支付安全。
住房和城乡建设部、中央网信办、教育部、科技部、工业和信息化部、公安部、民政部、人力资源社会保障部、交通运输部、商务部、文化和旅游部、国家卫生健康委员会、应急部、市场监管总局、广电总局、体育总局	2021年4月6日	《关于加快推进数字家庭建设 提高居住品质的指导意见》（建标〔2021〕28号）	第四章“完善数字家庭系统”第四章中提出：强化网络和数字安全保障。数字家庭系统应同步规划、同步建设、同步使用网络安全技术。按照法律法规规定和国家强制性标准要求，采取技术等措施，确保数字家庭系统安全稳定运行，防止信息泄露、篡改、丢失、确保收集、产生数据和个人信息安全。遵守密码应用规定，形成安全可靠完整的产业生态系统。
国家卫生健康委员会办公厅、国家中医药局办公室	2020年9月27日	《关于加强全民健康信息化体系建设的重点任务》（国卫办规划发〔2020〕14号）	第二章“全民健康信息化体系建设的重点任务”第四章“加强网络安全标准化建设”中第一点提出：完善行业网络安全标准体系。贯彻《中华人民共和国网络安全法》，推进网络安全等级保护、商用密码应用、关键信息基础设施保护等制度在行业落地实施。研究制定卫生健康行业网络安全技术、医疗卫生机构安全能力评估、关键信息基础设施识别认定和保护等标准。

发文/起草单位	发文时间	政策文件	相关内容
交通运输部办公厅	2018年1月31日	《交通一卡通运营服务质量管理暂行办法（试行）》（交办运〔2018〕17号）	第八章“安全管理”第六十一条中提出：交通一卡通运营机构应当按照国家关于网络安全及商用密码管理的法律和行政法规相关规定，使用交通一卡通商用密码，承担国产商用密码应用，落实业务数据和信息的安全保护责任，保障交通一卡通信息安全。
财政部	2017年12月26日	《政务信息系统政府采购管理暂行办法》（财库〔2017〕210号）	第八条提出：采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，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。 第十二条提出：采购人应当按照国家有关规定组织政务信息系统项目验收。根据项目特点制定完整的项目验收方案。验收方案应当包括项目所有功能的实现情况、密码应用和安全审查情况。信息系统类项目，除设备类采购文件和采购合同约定的内容，必要时可以邀请行业专家、第三方机构或相关主管部门参与验收。

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	《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指导意见》（公网安〔2020〕1960号）	第二章“深入贯彻落实国家网络安全等级保护制度”第六条中提出：落实密码安全防护要求。网络运营者应严格落实《密码法》等有关法律法规规定和商用密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理方法和相关标准，在网络安全等级测评中同步开展商用密码应用安全性评估。
国家发展改革委办公厅	2020年7月9日	《关于加快落实新型城镇化建设补短板强弱项工作有序推进智慧城市化改造的通知》（发改高技〔2020〕530号）	第三章“重点方向”第四章中提出：健全网络安全防护体系，做好网络安全与智能化改造一体化推进。落实网络安全工作责任制要求，完善智能化改造网络安全管理制度规范。认真落实国家网络安全等级保护、网络安全审查、云计算采购服务、国家密码管理等有关规定，采购部署安全可靠的软硬件产品，具备与智能化水平相匹配的体系化安全防护能力。
教育部办公厅	2020年2月26日	《2020年教育信息化和网络安全工作要点》（教科技厅〔2020〕1号）	第三章“重点任务”第五条“全面推进教育治理能力提升行动”中第十五点提出：加强教育系统密码应用与管理。落实《教育行业密码应用与创新发展实施方案》，推进密码基础设施和支撑体系建设，有序推动教育重要业务信息系统开展密码应用安全性评估。完善教育数字认证（CA）基础支撑体系建设，推动国家教育管理信息系统密码应用，提升系统安全和数据安全。
水利部办公厅	2020年2月14日	《2020年水利行业密码应用工作要点》（办信总〔2020〕22号）	第一章“水利行业密码应用”第一条“水利行业密码应用”中第二点提出：推进商用密码应用。组织宣贯《中华人民共和国密码法》，开展水利行业密码应用专题调研。出台推进商用密码应用具体措施。落实《水利行业密码应用与创新发展实施方案（2018-2022年）》，持续推进三峡水利枢纽、南水北调工程等重要水利基础设施和国家水运管理系统等重要信息系统的密码应用。
交通运输部	2019年12月9日	《关于印发〈推进综合交通大数据发展行动计划（2020-2025年）〉的通知》（交科技发〔2019〕161号）	第三章“重点任务”第四条“加强大数据安全保障”中第十八点提出：完善数据安全保障体系。推进交通领域数据分类分级管理，加强重要数据和个人信息安全保护，制定数据分级安全管理、数据脱敏等制度规范。推进重要信息系统密码技术应用和重要软硬件设备自主可控。
国家能源局	2018年9月13日	《国家能源局关于加强电力行业网络安全基础设施建设的指导意见》（国能发安全〔2018〕72号）	第五章“加强行业网络安全基础设施建设”第十四条中提出：加快密码基础设施应用。在重要业务、重要领域实施密码保护。完善电力行业密码支撑体系，实现电力行业密码基础设施一体化管理。健全电力行业密码检测手段，开展密码应用安全性评估。深化商用密码在电力行业中的应用，促进密码技术与电力应用融合发展。

附录4 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¹

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
北京市	2021年5月	《政府投资信息化项目密码应用工作规范》	新建网络和信息系统应当采用国产密码进行保护,同步规划、同步建设、同步运行密码保障系统,定期开展密码应用安全性评估。已建网络和信息系统应当进行密码国产化改造,确保使用的密码算法和技术符合国家的法律法规和国家标准,使用的密码产品和服务通过国家密码管理部门的核准或许可。
	2019年4月	《关于在政府投资信息化项目建设中规范使用密码的通知》	项目实施单位要同步规划、同步建设、同步运行密码保障系统,定期开展密码应用安全性评估,确保不新增安全风险。
天津市	2021年12月	《天津市政务信息化项目建设管理办法》	市级政务信息化项目建设应当符合国家和天津市网络安全、数据安全、密码使用相关要求;项目建设部门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、同步运行密码保障系统并定期进行密码应用安全性评估。
	2020年7月	《关于切实做好政务信息化项目密码应用工作的通知》	政务信息化项目建设单位,在申报项目资金前应当按通知要求向密码管理部门提交材料,进行密码使用合规性审核;在完成项目建设任务后,进行密评;在项目验收运行后,定期开展密评。

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
河北省	2020年11月	《关于进一步加强对非涉密政务信息系统密码应用与安全性评估工作的通知》(冀国密局字〔2020〕12号)	落实《河北省省级政务信息化项目建设管理办法》(冀政办发〔2020〕48号)要求,规范省内非涉密政务信息系统立项、实施、验收阶段密码保障系统建设、管理,落实“三同步一评估”要求。
	2020年4月	《河北省省级政务信息化项目建设管理办法》(冀政办发〔2020〕48号)	第十九条提出: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、同步运行密码保障系统并定期进行评估。 第三十七条提出:各相关部门应当严格遵守有关保密等法律、法规规定,构建全方位、多层次、一致性的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
	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》(冀国密局字〔2019〕2号)	贯彻落实中央文件精神,组织省内有关单位对某建设使用的重要信息系统开展密评,省密码管理部门对工作情况 and 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)	各预算单位要严格按照《密码法》及相关要求推进密码应用,涉及金融及重要领域的信息化项目要同步规划、同步建设、同步运行密码保障系统,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”第二十四条中提出:政务云服务提供方和政务云使用部门要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规范的软硬件产品及密码,优先使用自主可控的软硬件产品,定期开展密码应用安全性评估。
	2019年9月	《山西省政务信息化项目建设应用管理办法》(晋政办发〔2019〕72号)	第五章“管理和安全”第三十七条中提出: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,严格落实等级保护和国家密码管理要求,同步规划、同步建设、同步运行密码保障系统并定期评估,切实保障政务信息系统安全稳定运行。
内蒙古自治区	2023年1月	《内蒙古自治区“十四五”期间商用密码重点工作任务书》(内国密局发〔2023〕1号)	加强商用密码应用安全性评估和管理。推动关键信息基础设施、等级保护三级及以上信息系统、全区政务信息系统等同步规划、同步建设、同步运行密码保障系统,定期开展商用密码应用安全性评估;加强与政务信息化项目审批部门的工作协同,严格落实商用密码应用环境管理要求;加强对密评机构的指导和管理,探索建立用户评价机制,持续提升密评机构的能力水平;依据国家总体部署,按照科学布局、强化基础、考核认定的原则,适时培育商用密码应用安全性测评机构;持续优化“内蒙古自治区商用密码业务监管平台”功能,推进商用密码应用动态监测,加强商用密码应用信息归集管理,适时与国家平台对接。

*来源:中国密码学会商用密码应用安全性评估委员会

附录4 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	《自治区本级政务信息化项目建设暂行管理办法》(内发改高技字〔2022〕1963号)	第十二条第二款提出:备案文件应当包括项目名称、一、密码应用方案和密码应用安全性评估报告等内容。
	2022年11月	《内蒙古自治区数字经济促进条例(草案)》	第七十七条“安全保障”第六十五款中提出:网络运营者应当依法进行安全评估,采取数据测评、风险评估、安全漏洞分析和预警监测、网络安全等级保护、商用密码应用安全性评估、数据安全测评等安全技术措施,保障数据、网络、设施等方面的安全。
	2022年1月	《关于规范全区商用密码应用安全性评估结果备案工作的通知》(内国密局发〔2022〕1号)	本地区、本部门(行业)的网络与信息系统运营者为备案主体。网络与信息系统运营者应依照法律、法规、规章和国家、自治区有关规定,同步规划、同步建设、同步运行商用密码保障系统,规范开展密评工作,履行备案程序。
	2021年11月	《关于做好自治区本级政务信息化项目商用密码应用安全性评估工作的通知》(内国密局发〔2021〕7号)	一、本区新建政务信息化项目要依照国家商用密码管理应用相关法律法规和标准规范要求,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评估。 二、本区新建政务信息化项目在编制项目建议书、可行性研究报告和初步设计时,要同步将密码应用建设内容并编制密码应用方案。项目报建中途验收时,要提供密码测评报告,报告结论未通过的,不得提速验收。
	2021年9月	《内蒙古自治区商用密码事中事后监管方案》(内国密局发〔2021〕5号)	1. 监管事项(1)非涉密关键信息基础设施、网络安全等级保护第三级及以上信息系统、国家政务信息系统等重要网络和信息系统中国商用密码应用的合规性、正确性、有效性; 4. 监管方式和检查频次:监管方式:现场检查和委托第三方检测机构检测相结合。检查频次:从非涉密关键信息基础设施、网络安全等级保护第三级及以上信息系统、国家政务信息系统等重要网络和信息系统中国商用密码应用,随机抽查比例为每年10%-20%,3年内已被随机检查、无违规行为的,不列入随机检查范围。对随机检查不合格的部门单位加大检查频次。
辽宁省	2021年6月	《辽宁省政务信息化项目建设管理办法》(辽财办字〔2021〕382号)	第三章“中微内容”第七节“工程建设其他经费”中提出:工程建设其他经费是项目单位依据相关法规规定和委、办、局项目委托和经费管理调查,聘请相关的第三方服务机构提供相应服务所产生的费用,包括项目咨询(设计)服务费、工程监理费、网络安全等级保护测评费、第三方测试费、密码应用安全性评估费等内容。

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	2020年10月	《关于进一步加强政务信息化系统密码应用与安全性评估工作的通知》(辽国密发〔2020〕26号)	该文件对辽宁省内非涉密政务信息系统立项、建设、验收等过程中使用密码和开展密评工作提出要求。
	2022年5月	《吉林省促进商用密码产业高质量发展行动计划》(吉国密发〔2022〕1号)	该计划提出:依法督促我省重要网络和信息系统运营者同步规划、同步建设、同步运行商用密码保障系统,定期开展商用密码应用安全性评估;加强关键信息基础设施安全防护,网络安全等级保护制度与商用密码应用安全性评估要求的衔接;规范数据分类分级保护、互联网平台和个人信息处理者的密码使用管理。
	2021年12月	《关于落实商用密码应用安全性评估结果备案工作的通知》(吉国密办〔2021〕21号)	各地区、省直各部门网络与信息系统运营者依照法律、法规、规章和国家有关规定,同步规划、同步建设、同步运行商用密码保障系统,规范开展密评工作。 严格履行备案程序。各地区、省直各部门网络与信息系统运营者自密评报告出具之日起30日内,填写《网络与信息系统密评备案信息表》,连同密评报告报送商用密码管理局备案。各地区商用密码管理部门负责指导、汇总报送本地区网络与信息系统备案工作。
	2021年6月	《吉林省政务信息化建设“十四五”规划》(省政府办〔2021〕8号)	第十一章“建设安全可靠的管理保障体系”第一节“健全安全管理和应急工作机制”中提出:严格落实网络安全法律法规和政策标准要求,推动政务云平台获得安全认证,政务信息系统基础信息安全等级保护、风险评估、商用密码等有关规定,推动自主可控信息化产品和国产密码在相关领域的应用,提升密码基础支撑能力,确保政务系统建设自主可控、安全高效运行。
	2020年10月	《关于进一步做好政务信息化系统密码应用与安全性评估工作的通知》(吉国密办〔2020〕16号)	政务信息系统规划、建设、运行阶段,项目建设单位要严格落实国家密码管理局有关规定和标准要求,同步规划、同步建设、同步运行商用密码保障系统,并定期进行评估。 委托开展商用密码应用安全性评估的,应从《商用密码应用安全性评估试点机构目录》中选择评估机构。 商用密码应用安全性评估工作相关材料需报省密码管理局备案。
吉林省	2020年9月	《吉林省政务信息化项目建设管理办法》(吉国密办〔2020〕9号)	第一章“总则”第五款中提出:省密码管理局负责政务信息化系统密码应用的指导、监督和检查工作,指导项目建设单位按照要求采用密码技术、密码产品、密码服务,并定期开展商用密码应用安全性评估,确保政务信息系统运行安全和政务信息资源真实完整的数据安全。

附录4 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3月	《关于规范商用密码应用安全性评估结果备案工作的通知》	旨在规范和优化黑龙江省密评备案程序,要求网络与信息系统运营者,应同步规划、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密评工作,履行备案程序。自密评报告出具之日起30日内,填写《网络与信息系统密评备案信息表》,送网信部门备案。
	2021年12月	《黑龙江省“十四五”数字政府建设规划》(黑政发〔2021〕17号)	第四章“夯实四大数字基础支撑底座”第四节“构建全省一体化安全防护体系”第一节“提升安全保障能力”中提出:完善密码基础设施,建立信任服务体系,为资源安全利用和行为可信提供支撑,强化安全防护技术支持能力。加强数字政府密码应用服务能力,同步规划、同步建设、同步运行密码保障系统,推进政务信息化系统密码改造工作,并定期进行评估。
	2021年4月	《黑龙江省省级政务云管理暂行办法》(黑政办发〔2021〕17号)	第一章“总则”第六条中提出:省政务云按照国家标准管理有关法律法规和标准规范要求,同步规划、同步建设、同步运行密码保障系统。
	2020年11月	《关于进一步加强政务信息系统密码应用与安全性评估工作的通知》	旨在推动和加强黑龙江省政务信息系统密码应用与安全性评估工作。要求我省非涉密政务信息系统建设单位同步规划、同步建设、同步运行密码保障系统并定期进行密评应用安全性评估,保障密码应用与安全性评估经费,配备密码保障系统管理和运维人员。
上海市	2022年8月	《上海市市级数字化项目支出预算管理暂行办法》(沪经信信〔2022〕535号)	明确将密码产品、密码服务列入建设费,该建设费项目的支出范围,中报数字化项目应当严格落实密码应用要求,将密码应用情况作为建设费项目评审重点之一。项目实施时落实密码应用要求。项目验收时需提供密码应用测评报告。
	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”中提出:对于涉及国家安全和公共利益的重要网络和信息系统,包括涉密的关键信息基础设施、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,以及法律、行政法规和国家有关规定要求使用商用密码进行保护的其他网络和信息系统,应当落实密码有关法律法规、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	《上海市政务云管理暂行办法》(沪府办规〔2022〕6号)	政务云服务商负责建立健全安全防护工作制度,提供安全可信的产品和服务,做好政务云的安全监测和防护工作,定期开展网络安全等级保护测评与密码应用安全性评估,保障政务云安全稳定运行。 政务云主管部门、政务云运行管理单位和使用单位应当严格落实国家网络安全和商用密码应用要求,采取安全措施,并与政务云同步规划、同步建设、同步运行网络安全体系与密码保障体系。

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	《上海市电子政务云政务移动办公信息系统密码应用建设指南(暂行)》	可用于指导政务移动办公信息系统的责任单位规范开展密码应用与安全性评估工作,也可供系统集成单位、密码应用支撑单位和商用密码检测机构参考。各级地方政务移动办公信息化建设、使用、管理单位也可参照《指南》开展相关工作。
	2022年2月	《关于进一步加强我市电子政务云及上云信息系统密码应用与安全性评估工作的通知》	加强上海市电子政务云及上云信息系统密码应用与安全性评估工作。
	2021年5月	《关于规范和加强我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、工作实施流程和保障措施,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	《关于进一步规范和规范关键信息基础设施密码应用工作的通知》	规范和加强上海市关键信息基础设施密码应用与安全性评估工作。
	2022年4月	《省政府关于加快统筹推进数字政府高质量建设的实施意见》(苏政发〔2022〕44号)	第五章“筑牢网络安全数据安全防护墙”第十六条“严格执行安全管理制度”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保护、数据分类分级保护、密码应用管理等制度。
江苏省	2022年3月	《关于规范密码应用安全性评估结果备案工作的通知》(苏密码局字〔2022〕7号)	进一步规范省各有关部门、单位的密评与备案工作,明确密评和备案工作情况将作为网络安全工作责任制落实情况有关密码管理考核依据。
	2021年4月	《江苏省省级政务信息化项目建设管理办法》(苏政办发〔2021〕24号)	第三章“建设和资金管理”第十八条中提出:项目建设单位应当落实国家和省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	《江苏省政务信息化项目密码应用与评估备案指南(试行)》(苏密码局字〔2020〕43号)	该文件提出政务信息化项目密码应用与评估备案工作的要求和具体流程。

附录4 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⁴

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
浙江省	2022年9月	《关于对密评结果开展审查工作的通知》	对自2022年1月起至2022年12月底之前全省开展的密评项目,重点对各地各单位新建等保三级以上政务信息系统、《浙江省密码应用与创新发展实施方案》涉及的重要网络与信息系统密评结果,逐项核查密评流程是否客观、密评实施是否规范有效、密评记录是否清晰准确等。
	2022年8月	《电子政务建设项目中报工作的通知》	建设项目应按照国家有关规定和标准明确网络安全保护等级及密评,设计和采取网络安全保护措施。非涉密项目方案中也应包含符合国家标准设计的密码应用设计方案。重要网络与信息系统项目应按要求规划商用密码应用安全性评估。新建项目网络安全预算不低于项目总投资5%。
	2022年7月	《浙江省人民政府关于深化数字政府建设的实施意见》(浙政发〔2022〕20号)	第五章“构建数字政府全方位安全保障体系”第二条“落实安全制度要求”中提出:严格落实相关法律法规制度,全面落实《浙江省公共数据条例》,健全数据归集、治理、共享、开放、授权使用、安全管理等制度。建立网络安全等级保护、涉密信息系统分级保护、密码应用安全性评估制度,完善网络安全标准规范。探索建立首席网络安全官制度。
	2022年3月	《关于深入开展密码应用安全性评估工作的通知》	2022年,各地各单位新建等保三级及以上政务信息系统,必须落实商用密码应用安全性评估要求;同步规划、同步建设、同步运行商用密码保障系统,选择经国家密码管理局认可、具备相关资质的检测机构开展密码应用安全性评估工作,并基本符合密码应用要求。
	2022年1月	《浙江省电子政务外网安全评估指标体系(试行)》	安全防护层面中要求:统一建设密码服务云平台,为本地区提供密码服务;对本地区网络安全等保三级及以上政务信息系统开展商用密码应用安全性评估。
	2021年12月	《关于规范商用密码应用安全性评估结果备案工作的通知》(浙密码发〔2021〕29号)	请各地市各部门指导督促本地区、本部门(行业)有关网络与信息系统运营者自密评报告出具之日起30日内,填写备案信息表并在规定期限内将表格与密评报告报送密码局备案;请各市密码管理部门定期收集汇总所在地市的密评结果备案信息,填写《密评备案信息汇总表》按季度报送省密码管理局。
	2021年10月	《关于加强浙江辖区私募基金密码应用工作的通知》(浙证监机构字〔2021〕120号)	辖区各经营机构应当于2021年底前,完成方案制定和评审。2022年12月底前,完成系统改造、安全性评估及收尾工作;辖区国有控股证券公司、期货公司、基金管理公司、独立基金销售机构应严格按照要求开展密码应用工作,鼓励民营和外资机构资源开展相关工作;辖区各经营机构应当积极参与证券业协会、期货业协会、基金业协会组织开展的密码应用专项培训。

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
安徽省	2023年1月	《数字安徽建设2023年重点工作安排》	加强基础网络、数据中心、工业互联网平台等关键信息基础设施的安全保护,定期开展网络安全等级保护和商用密码应用安全性评估。
	2022年10月	《安徽省政务信息化项目建设管理办法》(皖数安〔2022〕2号)	第四章“项目建设管理”第三十条中指出:项目建设单位应当按照国家密码管理有关法律法规和标准规范要求,同步规划、同步建设、同步运行密码保障系统并定期进行商用密码应用安全性评估。
	2022年度	《综合绩效考核依据》	根据《安徽省金融和重要领域密码应用与创新发展实施方案(2019-2022年)的通知》,本部门新建、改建、扩建(含规划和建设中)的非涉密信息系统无密码应用且未作出相应规划安排的扣0.5分。
	2021年12月	《关于规范商用密码应用安全性评估结果备案工作的通知》	项目建设单位应落实国家密码管理有关法律法规和标准规范的要求,使用商用密码进行保护,同步规划、同步建设、同步运行密码保障系统并定期进行商用密码应用安全性评估。
福建省	2022年12月	《福建省数字政府改革和建设总体方案》(闽政〔2022〕32号)	全面推进重要领域商用密码应用,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。
	2022年3月	《关于加强商用密码应用与安全性评估工作的通知》(闽密〔2022〕1号)	网络与信息系统建设单位应当同步规划、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。
	2021年11月	《福建省“十四五”数字福建专项规划》(闽政〔2021〕25号)	第八章“筑牢可信可靠的网络安全屏障”第二节“完善网络安全监管体系”中提出:全面落实网络安全等级保护国家标准,坚持“自主可控”原则,完善密码基础设施建设,健全密码应用安全评估机制。
	2017年11月	《关于在数字福建建设项目可研暨初设编写提纲增加重要领域密码应用章节的通知》(闽数字办〔2017〕14号)	增加重要领域密码应用独立章节,要求安全系统设计根据系统安全等级保护级别,按照《信息系统密码应用基本要求》进行设计。
江西省	2021年8月	《江西省电子印章管理暂行办法》(赣府厅字〔2021〕61号)	第六章“安全管理”第二十七条中提出:具备完善的信息安全防护措施,通过商用密码应用安全性评估,至少符合信息安全保护等级三级要求。
	2020年9月	《江西省政务信息化项目建设管理办法》(赣府厅字〔2020〕68号)	第三章“建设和资金管理”第十五条中提出:项目建设单位应当按照《中华人民共和国网络安全法》《中华人民共和国密码法》等法律法规以及密码机关安全管理等有关规定,建立网络安全和密码安全管理等制度,同步规划、同步建设、同步运行密码保障系统,定期开展网络安全检测与风险评估,保障信息系统安全稳定运行。

附录4 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⁵

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
山东省	2022年1月	《关于规范商用密码应用安全性评估结果备案工作的通知》(鲁密码字〔2022〕1号)	该文件对各市和省有关部门、单位开展评估结果备案工作作了具体要求。
	2021年7月	《山东省“十四五”数字强省建设规划》(鲁政发〔2021〕128号)	推动密码创新和融合应用,落实密码应用与安全性评估要求,构建政务系统密码服务保障体系。
	2021年1月	《关于促进山东省网络安全产业发展的指导意见》(鲁网办发〔2021〕1号)	第二章“主要任务”第二节“服务模式升级”中提出:推动网络安全企业向提供安全产品向提供安全服务和解决方案转变,支持专业机构和企业开展网络安全规划咨询、安全集成、风险评估、检测认证、密码服务和检测、威胁监测、应急响应、安全运维、安全培训等安全服务。
	2020年4月	《山东省政务云平台管理暂行办法》(鲁数字〔2020〕7号)	政务云节点服务商应严格落实网络安全、保密、密码等相关法律法规,建立安全管理规范,定期开展网络安全等级保护测评、——、商用密码应用安全性评估等工作。
河南省	2023年1月	《河南省非涉密政务信息系统安全建设指南(试行)》(豫政办〔2023〕1号)	要求建设单位应根据政务信息系统安全防护等级,明确密码应用等级及需求,并编制密码应用方案;政务信息系统于上线前和运行期间每年开展安全风险评估,安全防护等级三级及以上系统还应同时开展商用密码应用安全性评估工作,并依据评估报告进行整改。 要求运维单位应根据密码管理部门的安全通报,对政务信息系统进行风险排查和安全加固。 要求建设单位应依法通过政府采购方式确定承担密码应用安全性评估的单位,并直接签订合同,严禁层层转包分包。
	2023年1月	《河南省促进商用密码产业高质量发展若干政策举措》(豫发改数字〔2023〕13号)	支持商用密码在全省非涉密政务信息系统、关键信息基础设施、网络安全等级保护第三级以上网络建设中的应用,依法督促重要网络和信息系统建设单位同步规划、同步建设、同步运行密码保障系统并定期开展商用密码应用安全性评估,落实评估结果备案制度,强化重要网络与信息系统商用密码应用与安全性评估情况的执法检查。加强电子政务服务电子证照基础设施设施建设,积极稳妥推动电子印章、电子证照等领域密码应用,支持重点企业开展政务、金融、交通、能源、医疗等领域密码应用示范,遴选推广典型场景优秀密码应用方案,推荐申报国家级商用密码试点示范。
	2022年11月	《河南省网络安全条例》(2022年11月26日河南省第十三届人民代表大会常务委员会第二十六次会议通过)	第十九条提出:县级以上网信、公安等有关部门应当指导督促网络运营者落实关键信息基础设施安全防护、网络安全等级保护、数据安全保护、个人信息保护、密码应用等安全评估、云计算服务安全评估、网络信息安全经济手段等制度,落实相关国家标准的强制性要求,制定网络安全事件应急预案。

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
河南省	2022年10月	《河南省加快推进电子证照“四电”扩大应用和互认互认实施方案》(豫政办〔2022〕101号)	提高“四电”支撑系统、应用系统安全保障能力,严格落实网络安全等级保护、商用密码应用安全性评估等要求,增强系统入侵防护、数据备份等防护功能。
	2022年9月	《河南省大数据产业发展行动计划(2022-2025年)》(豫政办〔2022〕90号)	第三章“主要任务”第七节“构建安全保障体系”中提出:实施数据安全“铸盾”行动,定期开展关键设施和系统安全评估、风险评估,建设网络安全应急体系,依法落实密码保护数据安全,定期开展商用密码应用安全性评估,落实网络安全等级保护和保密等要求。
	2022年4月	《河南省政务数据安全管理办法》(豫政办〔2022〕39号)	第七条提出:网信部门负责统筹协调、检查指导和相关监督管理等工作。公安部门负责等级保护、日常巡查、执法检查、信息通报、应急处置等监督管理工作。保密、国家安全、密码管理、大数据管理、通信管理等部门按照本法和有关法律、法规、规章的规定,在各自职责范围内承担政务数据安全监管职责。 第十一条提出:政务部门在落实等级保护、密码应用等要求,定期开展政务信息系统等级保护和商用密码应用等安全性评估。
	2022年1月	《河南省“十四五”新型基础设施建设规划》(豫发改数字〔2022〕52号)	“推动新型基础设施全部纳入关键信息基础设施保护范围,确保网络安全防护设施与新型基础设施同步规划、同步建设、同步使用。”“健全网络安全监测预警响应机制,构建以密码技术为核心、多种技术相融合的网络安全保障体系,加强重要新型基础设施可信性保障。”“推广安全可信、自主可控的网络产品和服务,强化密码技术在重要新型基础设施中的应用。”“严格落实网络安全工作责任制,严格执行网络安全等级保护、密码应用安全性评估等相关政策法规和标准规范要求”
	2021年12月	《关于规范商用密码应用安全性评估结果备案工作的通知》(豫密码电〔2021〕55号)	根据《关于规范商用密码应用安全性评估结果备案工作的通知》(国密码字〔2021〕392号),对河南省区域内评估及备案工作进行部署安排,提出有关备案要求。
	2021年10月	《关于开展我省重要领域网络和信息系统商用密码应用安全性评估工作的通知》(豫密码电〔2021〕40号)	2021年10月,河南省密码管理局召开开展年度密评抽查,要求各单位对已建重要领域网络和信息系统开展商用密码应用安全性自查,并抽取部分系统进行评估。
	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》(豫密码局字〔2020〕335号)	根据国家密码管理局《关于进一步加强国家政务信息基础设施密码应用与安全性评估工作的通知》(国密码局〔2020〕119号),河南省密码管理局、发展改革委、财政厅、大数据管理局联合印发文件,就河南省非涉密政务信息基础设施应用与安全性评估工作提出“三同步一评估”、保障密码应用与安全性评估经费、配备密码保障系统管理和运维人员等要求。

附录4 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⁶

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	2022年12月	《湖北省商用密码应用安全性评估工作指南(2022版)》	为更好指导非涉密关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统密码应用与安全性评估工作,汇编相关法律法规与政策文件、密码应用标准规范、应用方案示例、常见问题解答,形成《湖北省商用密码应用与安全性评估工作指南(2022版)》。
	2022年8月	《关于印发深化数据赋能扩大“免证明”应用领域工作方案的通知》(政办发〔2022〕42号)	加强电子证照应用安全监管,落实国家相关法律法规要求,完善电子证照管理规章制度,加强电子证照制度、归集、存储和使用环节的信息安全管理,防范未经授权擅自调用、留存电子证照等风险。对涉及个人隐私的证照数据,严格落实持证主体认证授权机制,充分保障持证主体的知情权、决定权。各地要加强数据安全自查和监管,强化电子证照数据和应用接口的安全防护,严格遵守网络安全等级保护制度规定,强化国产密码应用和安全性评估,主动感知发现并及时处置异常调用、非法访问等情况。
	2021年12月	《关于规范全省商用密码应用安全性评估结果备案工作的通知》(鄂密局发〔2021〕3号)	各地区、各部门(行业)有关网络与信息系统运营者应按照法律、法规、规章和国家有关规定,同步规划、同步建设、同步运行密码保障系统,规范开展密评工作,履行备案程序。
	2021年8月	《关于进一步加严政务信息系统密码应用与安全性评估工作的通知》(鄂密局发〔2021〕2号)	新建、扩建、改建以及通过政府购买服务产生的政务信息系统,项目建设单位应当同步规划、同步建设、同步运行密码保障系统并定期评估,采用符合国家标准的密码算法、技术,使用具有《商用密码产品认证证书》的密码产品和国家主管部门许可的密码服务。密码应用方案及密码应用方案评估报告是项目立项环节的必备材料,结论为“符合”或“基本符合”的密码应用安全性评估报告是项目验收环节的必备材料。未进行密码应用安全性评估或评估不合格的政务信息系统,不得继续投入运行。
	2020年7月	《关于印发湖北省数字政府建设总体规划(2020-2022年)的通知》(鄂政发〔2020〕12号)	加快安全管理系统建设,建设省市县三级全域安全态势与预警处理、云安全能力平台、安全数据分析平台、终端安全管理系统、攻防演练平台、密码支撑体系等。强化自主可控技术支撑,根据国家法律、政策法规,文件要求采用国产密码及自主可控的技术和产品,建设数字政府国产密码基础支撑体系,开展国产密码应用安全性评估工作,建立健全密码应用及自主可控安全性评估审查制度,推动云操作系统、数据库、中间件、大数据等方面国产化替代进程,推动安全可靠技术和产品在重要领域的应用。
	2018年9月	《湖北省政务信息化项目建设管理办法》(鄂政办发〔2018〕59号)	第三章“安全管理”第十三条中提出:项目建设单位应开展网络与信息安全风险评估,严格落实等级保护、分权保护和密码管理的要求,同步规划、同步建设、同步运行密码保障系统并定期评估,切实保障政务信息化项目安全稳定运行。

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	《关于促进电子政务协调发展的实施意见》(鄂政办发〔2015〕95号)	完善安全防护体系,按照密码应用规范的要求,构建全省电子政务安全防护体系,制定统一安全策略,划分安全域,保障基础信息网络、重要信息资源、重点业务系统和信息安全基础设施的安全。推动信息基础设施体系建设,建立符合国家相关标准规范的统一认证、授权管理,可信时间等安全基础设施,加大自主可控信息安全产品应用,强化安全保密意识,加强日常安全管理,落实密码管理相关主体责任。
	2022年3月	《政务信息化项目网络安全审查规范》(DB43/T 2313-2022)	第五章“审查合规性自查”第一节“方案编制”中提出:建设单位应对项目安全需求进行分析,并根据安全需求组织编制项目安全设计方案。安全设计方案应包含网络安全体系总体设计方案、密码应用方案、数据安全保护方案。
湖南省	2020年8月	《湖南省省直单位政务信息系统项目建设管理办法》(湘政办发〔2020〕34号)	第三章“建设和资金管理”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。未进行密码应用安全性评估或评估不合格的项目,不得通过项目验收,不得投入运行。
	2023年2月	《关于印发〈广东省促进密码产业高质量发展行动计划〉的通知》(粤密局发〔2023〕2号)	广东省密码管理局等16个部门联合印发该行动计划,进一步强调“重要网络和信息系统运营者同步规划、同步建设、同步运行密码保障系统,定期开展商用密码应用安全性评估并及时对结果进行备案”等要求。
	2022年12月	《关于进一步规范商用密码应用安全性评估试点工作通知》(粤密局发〔2022〕13号)	按照国家密码管理局有关文件要求,为进一步规范商用密码应用安全性评估试点工作,明确评估流程及监管工作要求等,广东省密码管理局印发该通知。
	2021年12月	《关于规范商用密码应用安全性评估结果备案工作的通知》(粤密局发〔2021〕7号)	按照国家密码管理局有关文件要求,为规范商用密码应用安全性评估结果备案工作,广东省密码应用推进工作协调小组办公室印发该通知。
	2021年3月	《广东省发展改革委广东省政务服务数据管理局关于印发〈广东省涉及固定资产投资的高级别政务信息化项目审批制〉的通知》(粤发改高技函〔2021〕566号)	在粤府办〔2020〕9号文件基础上,进一步明确涉及固定资产投资的高级别政务信息化项目的密码应用及商用密码应用安全性评估要求。
	2020年6月	《广东省政务服务数据管理局关于印发〈广东省省级政务信息化服务项目立项审批制〉的通知》(粤政数〔2020〕12号)	在粤府办〔2020〕9号文件基础上,进一步明确项目立项前对密码应用方案进行商用密码应用安全性评估等要求和流程。

附录4 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	《广东省政务服务数据管理局关于印发〈广东省政务服务信息化服务项目验收符合性审查细则〉的通知》(粤政数〔2020〕13号)	在粤府办〔2020〕9号文件基础上,进一步明确项目验收前对系统运行商用密码应用安全性评估等要求和流程。
	2020年6月	《广东省省级政务信息化项目商用密码应用工作指引》(粤密码协调组〔2020〕2号)	在粤府办〔2020〕9号、粤政数〔2020〕12号、粤政数〔2020〕13号文件基础上,广东省密码应用推进工作协调小组办公室印发该指引,进一步明确项目规划、建设、运行等阶段密码应用和商用密码应用安全性评估工作要求、流程;并根据最新政策和标准要求不断优化完善,分别于2021年9月修订《粤密码协调组〔2021〕4号》、2021年12月印发补充通知《粤密码协调组〔2021〕5号》、2022年9月修订《粤密码协调组〔2022〕6号》。
	2020年4月	《广东省人民政府办公厅关于印发广东省省级政务信息化项目管理办法的通知》(粤府办〔2020〕9号)	“涉及密码应用的项目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、同步运行密码保障系统并定期进行评估”。“不符合密码应用和网络安全要求的项目不予立项”。
	2022年9月	《关于加快数字化转型发展深入推动数字广西建设的实施意见》(桂发〔2022〕18号)	第一章“总体要求”第二条中提出:确保发展安全可控。统筹发展和安全,坚持促进发展与监管并重,建立健全安全管理体系、技术防护体系和协同监管体系,强化网络安全、关键信息基础设施安全、数据资源安全,全方位提升安全防护能力。 重点任务清单第四条“构建数字广西‘新基建’”中提出:健全网络安全等级保护、信息系统分级保护、密码应用安全性评估、风险评估、预警和应急处置制度,推动行业组织建立健全本行业的网络安全保护规范和协作机制。
广西壮族自治区	2021年12月	《广西政务信息化发展“十四五”规划》(公开版)(桂发改高技〔2021〕1196号)	创新密码技术和应用,强化密码安全管理和综合服务,加强密码应用测评能力建设,推进密码在政务信息化建设中全面有效应用。
	2021年3月	《广西壮族自治区政务信息化项目建设管理办法(试行)》(桂政办发〔2021〕21号)	第四章“建设和资金管理”第十九条中提出: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、同步运行密码保障系统并定期进行评估。
	2022年11月	《国家政务信息化项目验收管理规范(暂行)》(国数组办〔2022〕10号)	在政务信息化项目主管部门会同有关行业协会、发展改革委、密码局等相关单位组织竣工验收。明确商用密码应用安全性评估作为项目竣工验收的必备条件。密评报告作为项目验收必备材料。密码局专家代表在项目实施竣工验收会上具有一票否决权。

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	《海南省电子政务云密码服务管理办法(试行)》(琼数建〔2022〕46号)	进一步规范全省电子政务云上信息系统商用密码应用和管理,依托省电子政务云密码服务平台为全省各级政府部门提供集约高效的密码服务。
	2022年7月	《海南省政务信息化项目建设管理实施细则(暂行)》(琼数组办〔2022〕5号)	新建项目的网络安全设计应包括安全管理制度建设、入网安全评估、等级保护测评、渗透测试、安全加固等安全内容。运维类项目应部署规划网络安全等级保护测评、商用密码应用安全性评估、信息系统风险评估、应急响应、重要涉密保障等网络安全保障服务内容,保障信息系统安全稳定运行。
	2022年7月	《海南省促进商用密码应用和产业发展若干政策举措》(琼数组局学〔2022〕12号)	着眼自贸港建设风险防控需要,围绕自贸港封关运作准备工作大局,从统筹规范政务领域密码应用、推进重点领域和关键信息系统密码应用、鼓励科研创新和加强人才培养、支持培育企业和促进产业发展等几个方面共提出了15条针对性的政策举措。
	2022年6月	《海南省政务信息化项目投资编制标准(试行)》(琼数组办〔2022〕28号)	第二章“建设类项目投资估算编制”第二节“项目建设其他费”第七条“商用密码应用安全性评估费”中明确:商用密码应用安全性评估费的定义、费用范围、计价方法和标准等。
	2021年3月	《关于进一步明确省政务信息化项目建设密码应用有关要求的通知》(琼数组局学〔2021〕2号)	第五条、第七条中提出:新建、改建、扩建以及通过政府购买服务产生的政务信息化项目,项目建设单位在项目建设完成后,应委托评估机构对信息系统进行密码应用安全性评估。政务信息系统投入运行后,建设单位应按照密码管理有关法律法规要求定期委托评估机构对系统开展密码应用安全性评估,并根据安全需求、风险等级程度、系统环境变化以及对系统安全认识的深化持续改进密码保障措施。
重庆市	2020年12月	《海南省政务信息化项目建设管理办法》(琼府办〔2020〕38号)	第二章“规划和审批管理”第八条中提出:省级各部门产生的政务信息化项目,省大数据管理局应当按规定履行审批程序并向省发展改革委备案。备案文件应包括项目名称、建设单位、审批部门、建设目标及绩效指标、投资额度、运行维护经费、经费渠道、信息资源目录、信息共享开放、应用系统、等级保护或等保测评情况、密码应用方案和密码应用安全性评估报告等内容,其中改建、扩建项目还需提交前期项目第三方评估报告。
	2022年2月	《关于规范重庆市市级政务信息化项目密码应用有关要求的通知》(渝密局〔2022〕1号)	进一步明确市级政务信息化项目各阶段密码应用要求:项目规划阶段应按照相关标准编制密码应用方案,并对方案进行评审;项目设计阶段应严格按照通过评审的方案进行建设,建设完成后委托商用密码应用安全性评估机构进行评估。在商用密码应用安全性评估报告出具30日内报市密码局备案;项目运行阶段应开展定期评估、应急评估,统筹做好密码保障系统改进工作。

附录4 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	《重庆市中市级政务信息化项目管理办法》(渝府办发〔2021〕122号)	第四章“监督管理”第三十五条中提出:市级各部门应当严格遵守有关保密法律法规规定,构建全方位、多层次、一体化的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务数据资源真实交换的数据安全。
	2021年2月	《关于印发重庆市工业信息安全管理办法(试行)的通知》	第九条提出:主体责任企业负责本单位工业信息安全的主体责任,应结合实际做好本单位工业信息安全防护,建立健全工业信息安全责任制,负责本单位工业信息安全保障和应急处置工作,落实人、财、物保障,主体责任企业依法落实网络安全等级保护制度,开展定级备案、等级测评、商用密码应用安全性评估和安全建设整改等工作。
四川省	2023年2月	《关于委托开展商用密码应用安全性评估结果备案相关工作的通知》(川密码〔2023〕4号)	各市(州)密码管理局受省密码管理局委托,负责本地区密评结果备案的初审申报工作。驻川机构、省直部门以及中央、省属企事业单位规划建设的信息系统可直接报省密码管理局备案。
	2022年10月	《四川省省级政务信息化项目密码应用与安全性评估工作指南》(川密码〔2022〕18号)	对四川省省级政务信息化项目在规划阶段、建设阶段、运行阶段的密码应用和密评工作要求作出具体安排,用以指导各建设单位开展工作。
	2022年4月	《四川省一体化政务服务平台电子证照管理暂行办法》(川办规〔2022〕3号)	第五章“电子印章信息安全”第二十二条中提出:电子证照系统建设单位按照“谁建设、谁负责”的原则,落实网络安全等级保护制度和密码应用相关要求。电子证照系统建设单位应充分利用密码技术、生物特征技术以及其他必要的安全技术手段,加强证照中个人、持证主体身份认证,确保身份真实可信。
	2022年4月	《四川省一体化政务服务平台电子印章管理暂行办法》(川办规〔2022〕3号)	第一章“总则”第六条中提出:省一体化平台电子印章系统应当符合国家有关密码标准规范,应当通过国家密码管理部门认可的商用密码应用安全性评估。
	2021年10月	《四川省省级政务信息化项目管理办法》(川办发〔2021〕49号)	第四章“建设和运维管理”第三十一条中提出:建设项目由省委发展改革委组织竣工验收,验收资料包括密码应用安全性评估报告等材料。 第八章“安全管理”第四十九条中提出:省密码管理局应依法加强对政务信息系统密码应用的安全监管,指导监督项目单位规范密码应用和管理。 第八章“安全管理”第五十一条中提出:项目不符合密码应用和网络安全要求,或者存在重大安全隐患的,不得安排运维经费,项目单位不得新建、改建、扩建政务信息系统。

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9月	《四川省“十四五”数字政府建设规划》(川府发〔2021〕24号)	第四章“夯实数字政府建设基础”第五节中提出:落实关键信息基础设施保护制度和网络安全等级保护制度,建立重大项目网络安全风险评估机制,加强密码应用安全性评估工作。 建设密码技术支撑平台,规范、完善和深化密码在政务云平台等政务服务体系中的应用。 提升密码产品检测和质量控制能力,完善密码应用安全性评估审查机制,构建自主可控的密码认证测评体系。 推进基础设施网络密码应用,强化密码在信息惠民及社会治理中的应用,提升关键信息基础设施密码保障能力。
	2023年3月	《关于进一步规范商用密码应用安全性评估工作的通知》	指导各市州密码管理部门进一步细化职责,严格监督指导密评试点工作单位、密评机构,规范密评结果备案材料形式审查制度,建立完善密评结果备案材料复核制度,推动密评结果客观真实。
贵州省	2023年1月	《贵州省省级政务信息系统建设管理办法》	明确对省级政务信息系统密码应用“三同步一评估”作出明确要求,省大数据局组织相关部门,对项目建设单位报送的年度服务方案在相关政策符合性、可行性、软件架构及业务功能、数据来源建设与管理、密码应用、硬件部署方案、云资源占用合理性及投资预算等方面进行评审。
	2022年1月	《关于做好商用密码应用安全性评估结果备案工作的通知》	指导全省省直单位、中央在黔、人民团体等单位严格按照“三同步一评估”要求推进商用密码应用,规范开展商用密码应用安全性评估结果备案工作。
	2022年1月	《关于做好商用密码应用安全性评估结果备案工作的通知》	指导各市州密码管理部门按照分级管理要求,做好商用密码应用安全性评估结果备案管理工作,按时报送当地密评备案信息,指导督促本地网络与信息系统运营者按照“三同步一评估”要求,推进商用密码应用。
云南省	2022年5月	《云南省“十四五”电子政务发展规划》(云政办发〔2022〕37号)	第五章“筑牢主体化安全底座和标准规范体系”第一节“强化可控可控的安全与运维保障体系”中提出:推进国产密码应用,加强国产密码基础设施的建设和保护,推动关键基础设施保护、等级保护、分域保护、密码应用评估等信息安全测评工作常态化。
	2022年4月	《“十四五”数字云南规划》(云政发〔2022〕26号)	第八章“营造健康安全数字生态”第二节“健全网络安全体系”中提出:健全网络安全防护体系,落实信息安全等级保护,涉密信息系统分级保护及风险评估制度,定期开展网络安全专项检查与评估,规范、完善和深化国产密码应用,提升密码基础支撑能力,建立健全密码应用安全性评估审查制度。
	2022年4月	《云南省“十四五”新型基础设施发展规划》(云政发〔2022〕28号)	第六章“促进新型基础设施开放与安全”第二节“提升安全保障水平”中提出:规范密码应用和管理,促进密码产业发展,保障网络与信息安全,支持开展网络安全技术和产品研发。

附录4 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	《西藏自治区非涉密政务信息系统商用密码应用与安全性评估工作指南(试行)》(藏密局发〔2022〕3号)	该文件用于指导和规范西藏自治区非涉密政务信息系统商用密码应用与安全性评估工作,明确了商用密码应用编制及评审、信息系统商用密码应用安全性评估、商用密码应用安全性评估备案等业务流程和管理要求。
	2022年4月	《西藏自治区政务信息化项目建设管理办法》(藏政办发〔2022〕14号)	第三章“建设和资金管理”第十五条中提出:项目建设单位应当落实国家密码管理有关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。
	2021年12月	《关于规范商用密码应用安全性评估结果备案工作的通知》(藏密局发〔2021〕4号)	该文件提出商用密码应用安全性评估结果备案的具体要求。
陕西省	2023年2月	《关于征求陕西省政府建设2023年工作要点(征求意见稿)》	第四章“全面加强网络安全的坚固防线”第十五条“完善安全管理制度规范”中提出:完善各级政务网络安全管理制度规范,制定……密码应用等相关安全测评。
	2022年9月	《陕西省省级政务信息化建设项目专项资金管理办法》	进一步加强对省级政务信息化建设项目专项资金管理,将密码应用安全性评估经费纳入项目预算——确保专项资金安全运行、专款专用。
	2022年6月	《陕西省省级政务信息化项目建设管理办法(暂行)》(陕政办发〔2022〕19号)	第一章“总则”第三条中提出:省委网信办、省公安厅、省国家保密局、省国家密码管理局、省审计厅等按照职责分工,负责项目网络安全监管、等级保护、分级保护、密码评估、审计监督等相关工作。
	2021年10月	《陕西省人民政府办公厅关于印发政务信息化建设“十四五”规划的通知》(陕政办发〔2021〕27号)	第三章“主要任务”第二节“三大运行保障”中提出:加强政务数据全生命周期管理,制定完善政务数据安全管理制度和数据分类分级、共享开放、使用授权等管理制度,落实等级保护、商用密码应用安全性评估等合规性要求。
甘肃省	2022年4月	《甘肃省人民政府办公厅关于加快推进电子证照扩大应用领域和互认互认的通知》(甘政办发〔2022〕50号)	第二章“全面落实工作任务”第十条中提出:强化电子证照安全管理。各地各部门要做好电子证照系统日常运行维护,定期开展网络安全等级保护测评、密码应用安全性评估等工作。
	2021年12月	《甘肃省数字政府建设总体规划(2021-2025)》(甘政办发〔2021〕113号)	第四章“主要任务”第五节“推进体系建设,完善数字政府运行新机制”第二条“构建可信可控的安全保障体系”中提出:落实安全技术手段支撑,逐步推进安全技术手段建设,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,形成覆盖政务云、网、大数据底座、政务业务应用的安全保障技术支撑能力。
	2021年9月	《甘肃省“十四五”数字政府创新发展规划》(甘政办发〔2021〕88号)	保障数据安全,落实等级保护、密码应用、安全测评、密码测评、电子认证、应急管理等相关制度。

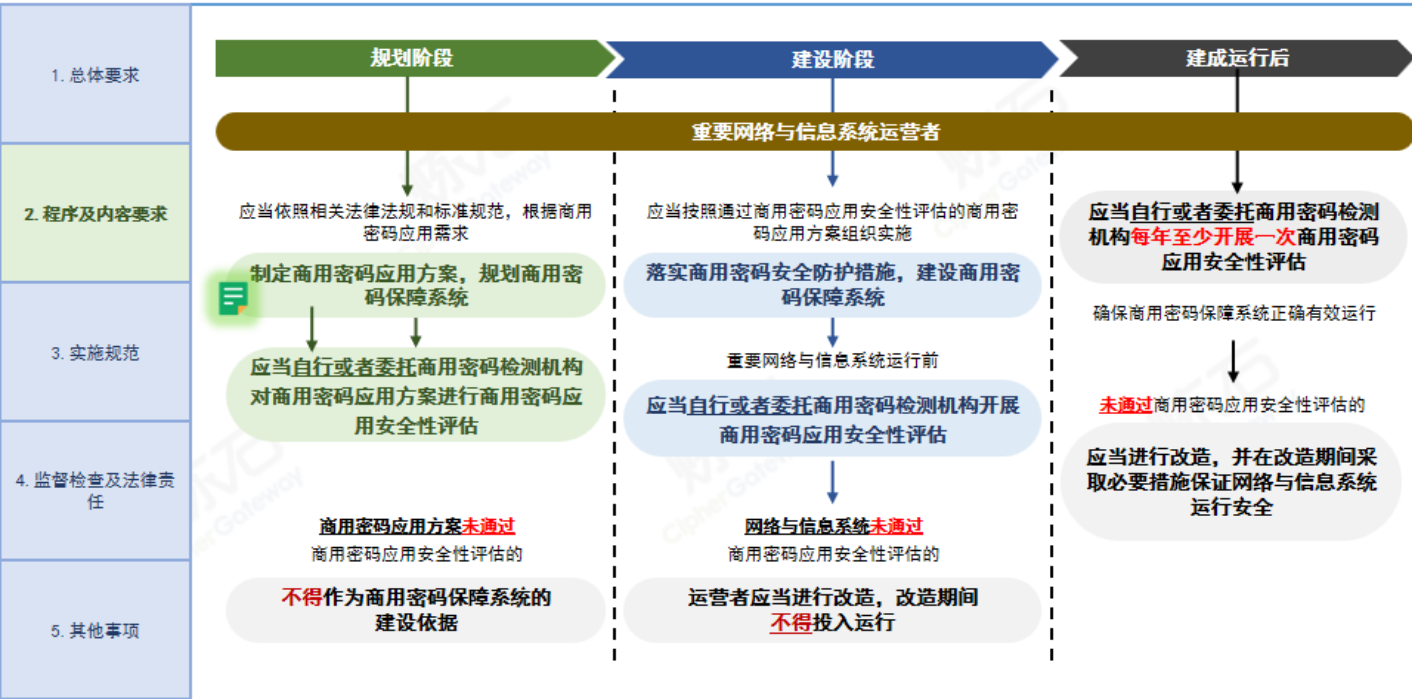
省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
青海省	2020年5月	《关于印发青海省省级政务信息化项目建设管理办法的通知》(青政办发〔2020〕38号)	第三章“建设和资金管理”第十八条中提出:项目建设单位应当落实国家网络安全和密码管理有关法律法规和标准规范的要求,同步规划、同步建设、同步运行网络安全和密码保障系统并定期进行评估。 第四章“监督管理”第三十三条中提出:各部门应当严格遵守有关保密等法律法规规定,构建全方位、多层次、一致性的防护体系,按需求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
	2023年1月	《关于进一步规范全省商用密码应用安全性评估工作的通知》	进一步强化密评主体责任,加强对密评实施活动的监督,规范密评结果备案工作,严格开展形式审查,鼓励商密协会发挥作用,加强行业自律,促进行业健康发展。
宁夏回族自治区	2022年5月	《关于进一步规范全区政务信息化项目商用密码应用和安全性评估的通知》(宁密局发〔2022〕1号)	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,使用商用密码进行保护,同步规划、同步建设、同步运行密码保障系统并定期开展商用密码应用安全性评估。 在项目规划阶段,应制定密码应用方案,并委托评估机构对方案开展商用密码应用安全性评估。未通过密评的密码应用方案,不得作为密码保障系统的建设依据;项目建设完成后,应委托评估机构开展商用密码应用安全性评估。信息系统投入运行后,项目建设单位应委托评估机构每年对系统开展商用密码应用安全性评估,确保密码保障系统正确有效运行。关键信息基础设施和网络安全等级保护第三级系统应在2022年底前完成,未通过商用密码保障系统并通过评估的,第二年不予安排运维经费,并暂停安排除商用密码保障系统建设完善之外的信息化项目。
	2021年12月	《关于规范我区商用密码应用安全性评估结果备案工作的通知》(宁密局发〔2021〕1号)	网络与信息保密系统备案主体应为各地区各部门网络与信息保密系统运营者,各责任单位务必高度重视,认真履行密码安全主体责任,明确密码安全负责人,按要求开展密评、备案和密码应用整改,配合密码管理部门和有关部门的安全检查。
	2021年8月	《宁夏电子政务建设十四五规划意见》	1)严格落实商用密码应用安全性评估制度,强化全网、全业务、全业务的电子政务综合安全防护。2)升级优化电子政务信息基础设施,为电子政务资源安全利用和可信提供安全支持保障。3)完善电子政务密码保障体系,促进电子政务公共云平台密码服务能力建设,为云上应用提供集约化密码服务,实现密码在电子政务系统中的有效应用。

附录4 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	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)	网络运营者要认真贯彻落实《中华人民共和国密码法》等相关法律法规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”的要求正确、有效采用密码技术对网络系统运行保护,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)以上网络运营者要尽快按要求进行整改。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防护措施,在网络安全等级测评中同步开展密码应用安全性评估,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性评估工作的通知》(新机发明电[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级以上的网络和信息系统应开展商用密码应用安全性评估。其中采取租赁云平台部署的信息系统(如门户网站等)应独立可进行评估;采取租网或终端方式接入上级部门建设的重要信息系统的,需具备本地接入用户、系统运维管理等实质权限,或在本地进行系统数据汇集、系统分中心等部署等实质控制行为,应独立进行评估。”“确保客观。各地各部门应采取直接委托具备资质的第三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自主开展工作,不得影响评估结果。”
	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“监督保障”第三十八条中提出:公共数据提供部门、公共数据使用部门、平台建设运维管理部门应遵循“谁提供、谁负责,谁使用、谁负责,谁流转、谁负责”的原则,按照国家信息安全等级保护、数据安全分类分级管理、密码应用安全保护要求,在公共数据资源开放过程中加强安全评估、访问控制、授权管理、全流程审计等方面的安全管理和防护。
	2021年2月	《新疆维吾尔自治区密码管理局关于深入贯彻落实密码法进一步健全完善自治区密码应用和管理工作机制的指导意见》(新密局[2021]4号)	第二节“建立完善密码应用工作报告机制”中提出:“责任单位要将密码应用管理工作纳入项目建设关键环节,规划阶段:责任单位应依据密码应用有关标准,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评估论证,论证结果作为必要附件列入项目立项材料并报送本级密码管理部门备案。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性评估,评估结果作为项目验收重要依据并报送本级密码管理部门备案。运行阶段:定期开展商用密码应用安全性评估,评估报告报送本级密码管理部门备案。” 第四节“建设完善密码应用联合审查机制”中提出:“4.项目验收阶段。密码应用安全性评估报告是项目验收的必要条件。对于不符合密码应用和网络安全防护要求,或者存在重大安全隐患的政务信息系统,不得通过验收,项目建设单位不得新建、改建、扩建信息系统。”

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
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。 第二十八条提出:“……各部门应当严格遵守有关保密等法律法规规定,构建全方位、多层次、一致性的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。”
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》(新兵办发[2021]126号)	第七章“安全管理”第四十七条中提出:项目建设单位应落实国家网络安全、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保密设施建设,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。

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

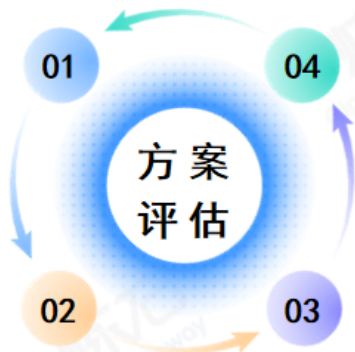
分析商用密码应用**流程和机制**是否具备**可实施性**、商用密码**保护措施**是否达到相应的商用密码**应用要求**、**相关描述**是否详尽。

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

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

01

划定评估范围



对照商用密码应用方案，了解网络与信息系统基本情况，准确划定评估范围。

02

确定评估指标及对象



确定评估指标及评估对象，论证编制商用密码应用安全性评估实施方案。

03

现场评估



依据商用密码应用安全性评估实施方案，开展现场评估，做好数据采集和信息汇总，研判商用密码保障系统配置及运行情况。

04

编制评估报告



根据客观凭据逐项对评估指标进行判定，编制形成商用密码应用安全性评估报告。

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

对**网络与信息系统**的重要数据进行备份；

设备清单和网络拓扑

提供**完整有效的网络与信息系统设备清单和网络拓扑**；

运营维护记录

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**；

管理入口

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**，并配合进行数据采集；

管理员

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；

其他事项

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的保存期限不得少于6年。			

重要网络与信息系统运营者应向管理部门备案评估报告

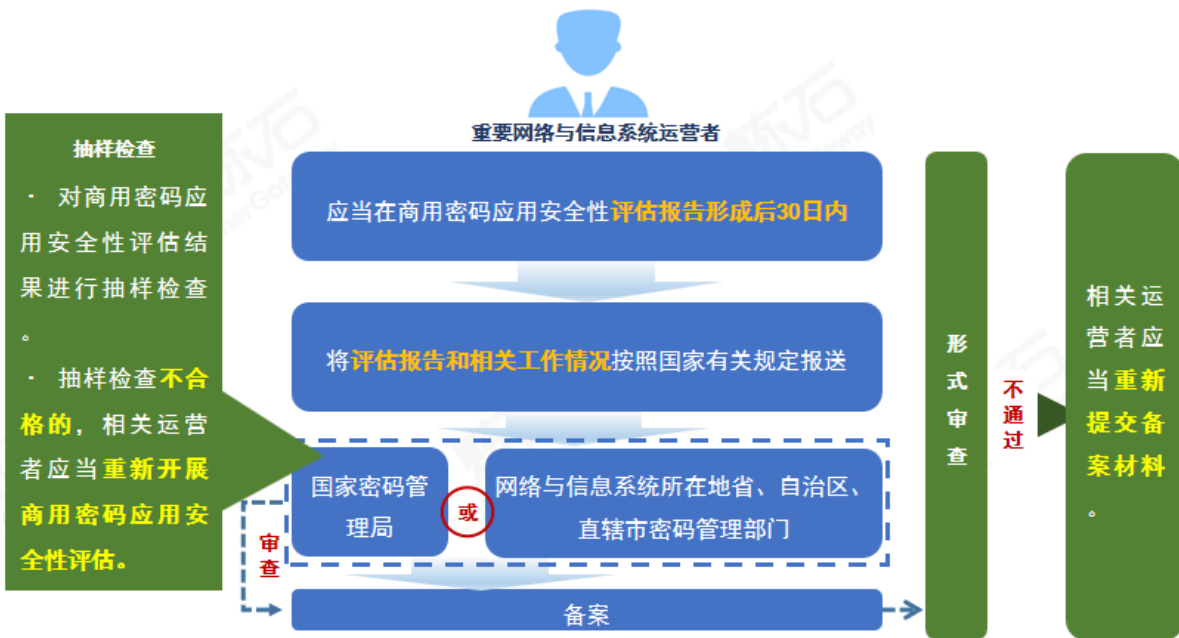
1. 总体要求

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、直辖市密码管理部门应当按季度向国家密码管理局报送本地区商用密码应用安全性评估工作开展情况。

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；	
		(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；	
3. 实施规范		(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；	
		(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；	
4. 监督检查及法律责任		(八) 不符合相关要求自行开展商用密码应用安全性评估的。	
	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。
5. 其他事项	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。

1. 《国家密码管理局商用密码随机抽查事项清单（2024年版）》

2. 抽查依据中涉及的相关法规解读

01 《密码法》

02 《商用密码管理条例》

03 《商用密码检测机构管理办法》

04 《商用密码应用安全性评估管理办法》

3. 炼石免改造数据安全与密码应用实践



安全需求：内在风险、外部合规、增量价值

安全产业自身

数据安全产业发展阶段性（先发展再治理，今天已到拐点）、自身特殊性（经济学外部效应带来的密集法律法规），形成非线性增长驱动力。

内在风险：数据风险如影随形伴生数据处理

根据IBM最新发布的《2023年数据泄露成本报告》，数据泄露的平均成本创下**445万美**元的历史新高，较过去3年均值**增长了15%**。



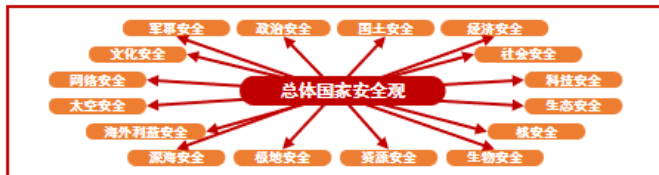
经济学外部效应：数据泄露给他人造成损害，对企业影响反而不大。解决办法是通过立法，让“防数据泄露”成为公共安全产品，类似环保。

外部合规：“五法一典”过程与结果双合规

网络安全法	个人信息保护法	数据安全法	密码法
网络安全等级保护条例 (征求意见稿)	关键信息基础设施安全保护条例	网络数据安全条例 (征求意见稿)	商用密码管理条例
等保	关保	数评	密评
信创			

信息技术产业

国际形势变化带来的空前安全需求，重要性（数字安全和几乎全部安全领域相文）和长期性（未来几十年新常态）。



二十大报告

加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。

健全国家安全体系，强化经济、重大基础设施、金融、网络、数据、生物、资源、核、太空、海洋等安全保障体系建设。

增量价值：“数据入表”让安全从成本走向价值



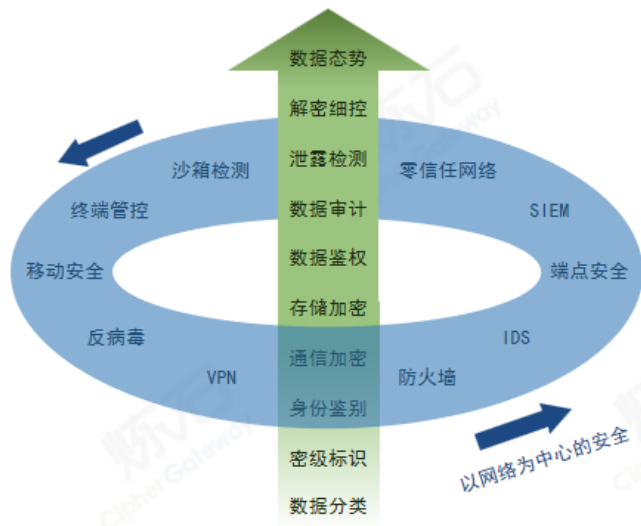
财政部《企业数据资源相关会计处理暂行规定》，将**数据入财务报表并体现其真实价值与业务贡献**，对数据资源确认范围和会计处理适用准则等作出规定，2024年1月起施行。

过去，数据通过提升运营效率间接为企业创利，而与生俱来的风险让数据成为企业不可忽视的“**表外负债**”。

现在，通过数据安全手段消减风险，在新会计准则下可以让数据成为企业实实在在的“**表内资产**”。

落地痛点：安全建设从网络到数据，安全和业务纠结缠绕难以改造

以数据为中心的安全



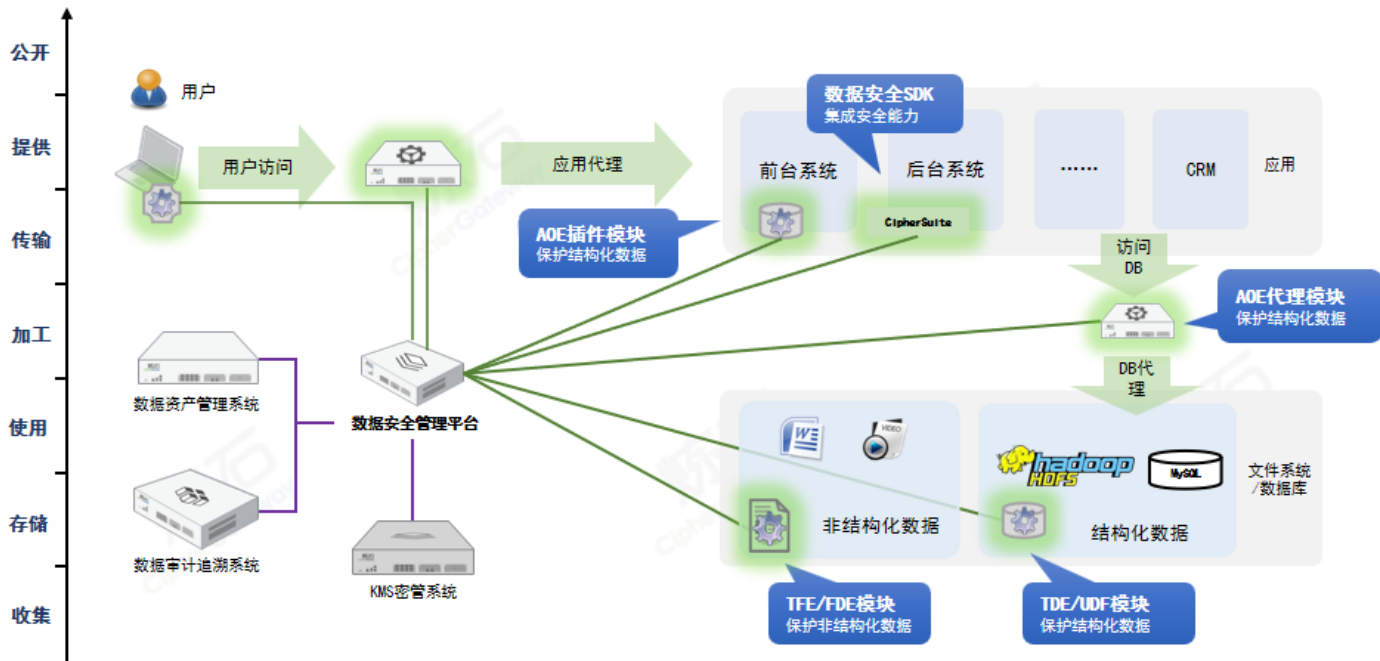
数据安全成为当前建设重点



数据安全建设面临“两难”：

- 数据保护体现为**面向应用的功能型安全需求**，要在应用中融合实现，**但改造存量应用成本高、风险大、周期长，新应用的业务开发与安全排期也不匹配，安全机制总是滞后或缺失**
- 而数据保护不落实，则合规风险越来越大、因泄露导致的业务风险会快速累积

敏捷部署：旁路平台结合主路控制面，免改造应用拦截数据施加保护



产品价值：将安全能力投送到复杂的数据处理流程中

免改造技术对流动数据的高覆盖率识别与控制，实现安全与业务有机融合



需求划分：整体数据安全包含“一实战、双合规”

实战是检验安全能力的唯一标准

实战对抗

HVV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



DSM
PIP
ABCD
PIP
CB
ABCD
APP

过程合规

商用密码应用安全性评估

合规

(过程之监管)

正确

(过程之技术)

有效

(结果导向)

结果合规

网信&市场监管：数据安全管理体系认证

网信&市场监管：个人信息保护认证

财政部：数据入表安全合规

BM&公安：工作秘密防护

国资委：商业秘密保护

【国标】数据安全能力成熟度认证

【国标】数据安全风险评估

密评合规

实战

数安合规

合规为表

数据安全
市场演进

实战为里

密评合规

实战

数安
合规

国密合规实践

一站式密改套餐敏捷交付

密码合规解析

最贴合业务

业务风险影响范围广，改造难度大
涉及核心的高风险项，且分值最高

属于密码应用层，含高风险项最多

密改落地由用户执行，无法绕过
所需密码产品会随着信息系统新增或变化，而扩容或调整

属于密码支撑层

密改落地不一定由用户执行，有可能属于IDC托管方、云服务商等
整体被评，可复用到被承载的每个信息系统

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	重要网络与信息系统（关基、等保三级、政务等） 每年至少一次

高风险项，一票否决

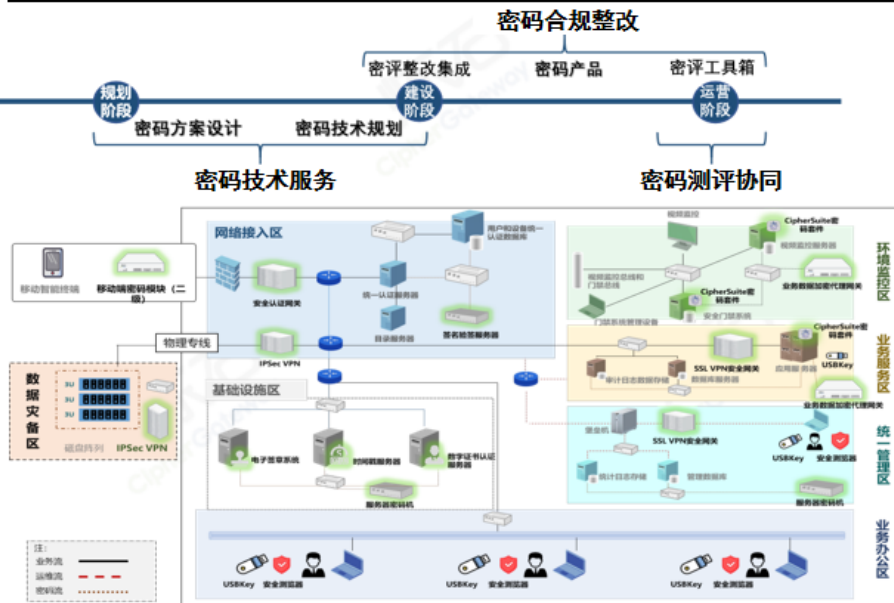
- 实体间未通过密码技术进行身份鉴别（网络和通信：无缓解措施）
- 未采用密码技术保证通信过程中重要数据的机密性
- 未采用密码技术建立安全的信息传输通道，如SSLVPN
- 未采用密码技术保证重要数据在存储过程中的机密性（无缓解措施）
- 未采用密码技术保证重要数据在存储过程中的完整性
- 未采用密码技术保证重要数据在传输过程中的机密性
- 未采用密码技术提供数据原发证据和数据接收证据（法律责任场景）
- 未建立密码相关管理制度
- 未制定密码应用解决方案、实施方案和应急处置方案，未通过评审
- 未采用密码技术对外部连接到内部的设备进行认证（第四级）

密码合规要点（以密码应用三级系统为例）

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	密码人员管理	密钥管理	建设运行	应急处置	密码软硬件	介质管理等制度		
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					30分	
应急处置	应急处置方案	及时上报						

炼石国密合规改造服务

炼石国密合规改造方案适用于政务、金融、交通、运营商、医疗、教育、工业、能源、水利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GM/T 0054和GB/T 39786中实现要求，为客户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A0E模块，非结构化数据TFE模块；

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。

密评合规产品：70分密改套餐

测评层面	测评单元	备注	满分	得分	密码产品
物理和环境安全 (10分)	身份鉴别	高风险	4.17	0.00	高风险可缓解
	电子门禁记录数据存储完整性		2.92	0.00	
	视频监控记录数据存储完整性		2.92	0.00	
网络和通信安全 (20分)	身份鉴别	高风险 (无缓解)	5.88	5.88	IPSec VPN安全网关 SSL VPN安全网关
	通信数据完整性		4.12	4.12	
	通信过程中重要数据的机密性	高风险	5.88	5.88	
	网络边界访问控制信息的完整性		4.12	4.12	
设备和计算安全 (10分)	身份鉴别	高风险	2.08	2.08	SSL VPN安全网关
	远程管理通道安全	高风险	2.08	2.08	
	系统资源访问控制信息完整性		1.46	1.46	密钥管理与数据加密 及认证平台
	重要信息资源安全标记完整性		1.46	1.46	
	日志记录完整性		1.46	1.46	
应用和数据安全 (30分)	重要可执行程序完整性、重要可执行程序来源真实性		1.46	0.00	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
	身份鉴别	高风险	4.05	4.05	
	访问控制信息完整性		2.84	2.84	
	重要信息资源安全标记完整性		2.84	2.84	
	重要数据传输机密性	高风险	4.05	4.05	
	重要数据存储机密性	高风险 (无缓解)	4.05	4.05	
	重要数据传输完整性		4.05	4.05	
	重要数据存储完整性	高风险	4.05	4.05	
安全管理 (30分)	不可否认性	高风险	4.05	0.00	仅限法律责任场景
	按得分80%计算		30	24	专业管理制度模板
合计			100	78.49	

密改四件套，轻松过密评

国密VPN网
关产品

解决网络和通
信20分、缓解
高风险

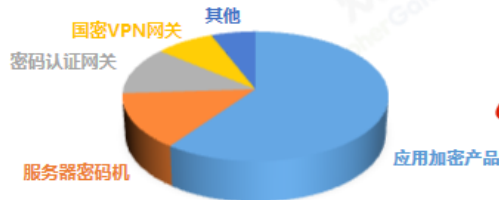
密码认证
网关产品

解决应用和数
据5分、缓解高
风险

应用加密
网关产品

应用和数据21
分、高风险，
设备和计算4分

服务器密码机
提供基础加解密算力与密管能力



免开发改造实现“应用和数据”机密性完整性

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

密码模块

密码模块

窃取数据

面向用户侧动态脱敏

密钥管理与数据加密及
认证平台

面向服务侧存储加密

非结构化数据

TFE文件加密

FDE全磁盘加密

明文

密文

明文

授权进程可
读取文件明文

未授权进程
只能读密文

挂载磁盘
或查后可
读取文件
明文

密文

密文

磁盘存
储密文

磁盘存
储密文

不影响业务人员使用、不影响DBA运维

示例

姓名	电话	年龄	注册时间
张三	13714	35岁	2020-01-24 09:05
李四	13723	32岁	2020-01-24 09:05
王五	13732	38岁	2020-01-24 09:05
赵六	13741	36岁	2020-01-24 09:05
刘七	13750	34岁	2020-01-24 09:05
张三	13759	33岁	2020-01-24 09:05
李四	13768	31岁	2020-01-24 09:05

应用查看脱敏后数据

示例

姓名	电话	年龄
张三	1371630482	非常密
李四	13750417164	非常密
王五	14735816218	非常密
赵六	10250726110	非常密
刘七	13156901590	非常密
张三	11965283955	非常密
李四	1877677924	非常密

应用看到密文

示例

NAME	VALUE	TYPE
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文

DBA工具查看脱敏数据

示例

NAME	VALUE	TYPE
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文
00000000000000000000000000000000	00000000000000000000000000000000	密文

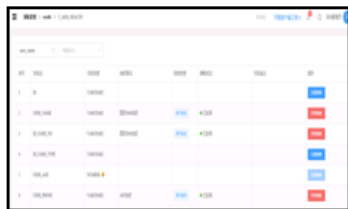
DBA工具查看密文

集中式管控，分布式保护，分阶段实施

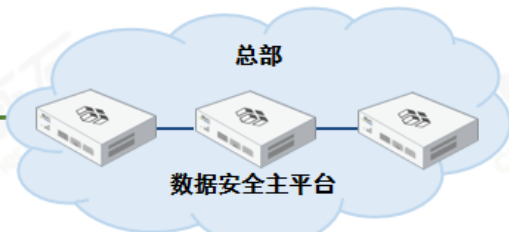
统一策略管理

集中式管控

统一密钥管理



配置



配置



分布式保护

.....



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

炼石
CipherGateway

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



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

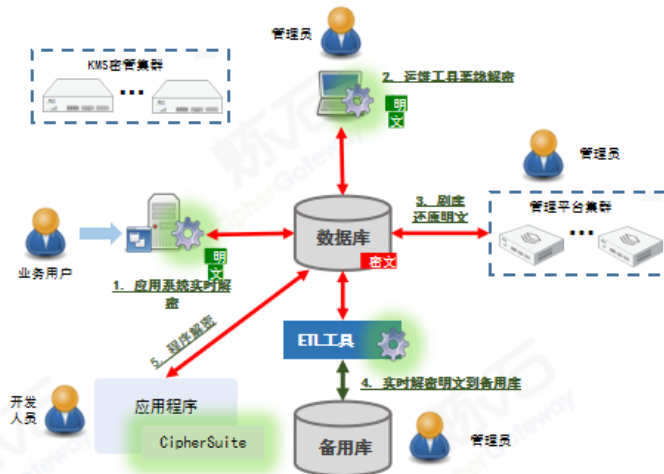
工作密钥（数据加密、数据MAC）

- 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】

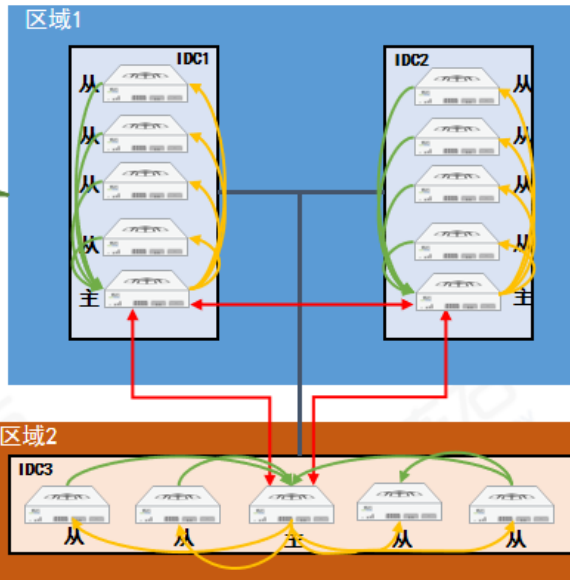
- 模块从平台获取规则后可缓存在内存中，当平台不可用也可正常运行
- 仅当模块所在服务重启时才需要从平台集群重取规则

【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

工业级实现：加密机制适应企业复杂场景

明密文标识确保加解密可靠

COMPLAIN_NO	PARTY_ID_NO	CONTACT_TEL
20150721000007	xOxVny30eLwC7PpPwLwW/a25g	wTtCpYze1mOxUG2
20150721000008	xOxM73eL/CbLwP/33J6ZOM2w	wTtdPyT/136Db9Wny
20150721000009	xT9VMS30eLwCPLwP/33J6ZOM2w	wTzP3yWw67CcdNq
20150721000010	mOxVny30eLwC7PpPwLwW/a25g	wOZQNC2FwC6Tsc4KEg
20150721000011	wOxVny30eLwC7PpPwLwW/a25g	wTtONCn9w4D75Se
20150721000012	wOxVny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000013	wOxVny30eLwC7PpPwLwW/a25g	wTtONCn9w4D75Se
20150721000014	xT9VMS30eLwCPLwP/33J6ZOM2w	wTtSN3C3c1n4OHuq7U
20150721000015	wOxVny30eLwC7PpPwLwW/a25g	wTtNn1eW4D7FUC
20150721000016	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000017	xOxVny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000018	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000019	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000020	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000021	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000022	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000023	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000024	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000025	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000026	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000027	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000028	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000029	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000030	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000031	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000032	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000033	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000034	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000035	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000036	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000037	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000038	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000039	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000040	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000041	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000042	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000043	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000044	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000045	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000046	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000047	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000048	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000049	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e
20150721000050	wT9Vny30eLwC7PpPwLwW/a25g	wTtdNye1Vn6Dr298e

- 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
d	其他	

姓名	性别	年龄	手机号	身份证号
张三	男	20	188 1111 2222	110102 1996 0102 3333
n1 n2			p1 p2 p3	ID1 ID2 ID3 ID4
n3			p4	ID5

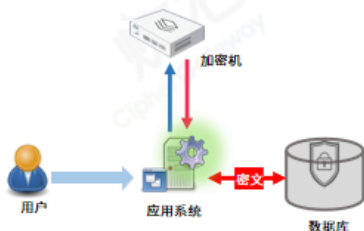
↓

密钥ID	n1, n2, n3	男	20	p1, p2, p3, p4	ID1, ID2, ID3, ID4, ID5
------	------------	---	----	----------------	-------------------------

- 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

技术对比：“应用和数据”密改典型路线

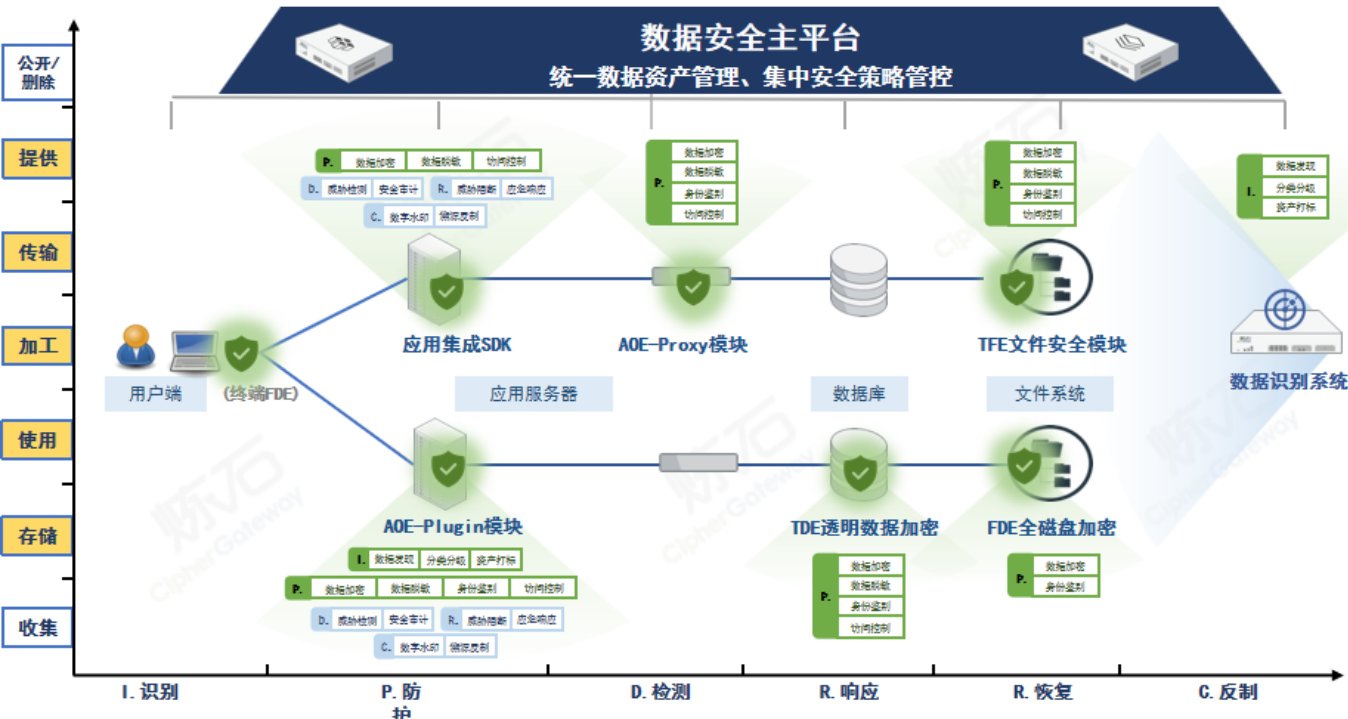
指标	轻改造应用的本方案	改造应用方案	数据库外挂安全方案
实施成本	实施工作量小，免改造应用代码	实施工作量大，需改造应用代码，集成加密机客户端SDK	实施工作量中，需针对目标数据库的每个版本做适配
可靠性	可靠性高，插件成为应用程序的一部分，不单独启进程，插件可靠性取决于应用自身可靠性	可靠性中，数据需要传输给集中部署的加密机进行加解密，形成性能瓶颈和单点故障风险	可靠性低，外挂模块需要在数据库服务器单独启进程，增加了单点故障风险，同时需要对数据库改表名、加规则
性能	性能高，基于高性能国密算法、脱敏算法	性能中，需要将数据传入传出加密机，额外增加网络延时	性能低，针对字段添加触发器和多层视图
兼容性	支持绝大多数数据库，与数据库解耦	支持绝大多数数据库，取决于SDK编程语言类型	仅支持Oracle等部分数据库，对国产数据库、NoSQL、乃至DB2、SQL Server等兼容性差
数据流	不改变原数据流转路径和网络拓扑，免改造模块原地加解密数据、脱敏数据	改变数据流转路径，明文先经过SDK传入到加密机，加密后将密文返回SDK，最终存入数据库	改变数据流转路径，明文先经过外挂模块传入到加密机，加密后将密文返回外挂模块，最终存入数据库
扩展性	可灵活扩展，统一可视化策略管理，横向覆盖更多应用，不影响已部署应用的加解密性能	扩展成本高，加密策略需要通过硬代码实现，任何策略改动，都需要改动代码，不灵活而且风险大	扩展成本中，需适配新数据库及改表名，对集中式加密资源增加压力，会分摊到已部署数据库的加解密算力
应用升级影响	不影响应用升级，加解密等功能与应用轻耦合	应用升级需要维护加密代码，加解密与应用代码紧耦合	应用升级要评估数据库，占用数据库服务器宝贵性能资源



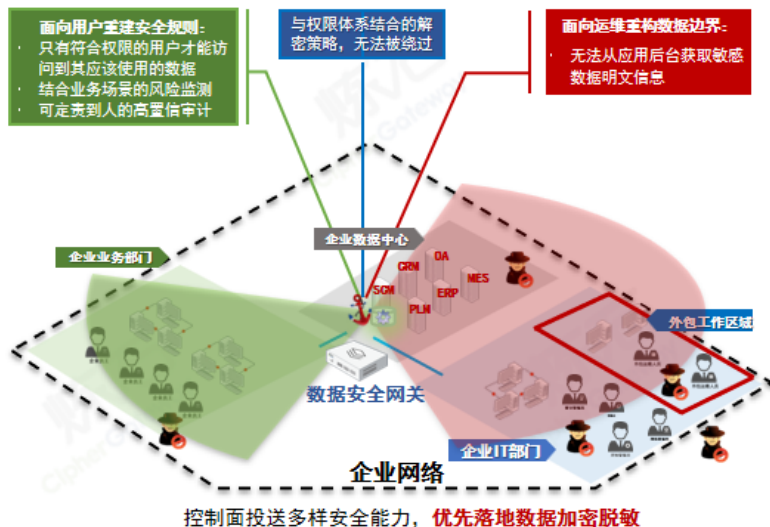
数据安全实战防护实践

基于产品与服务，事前事中事后全防护

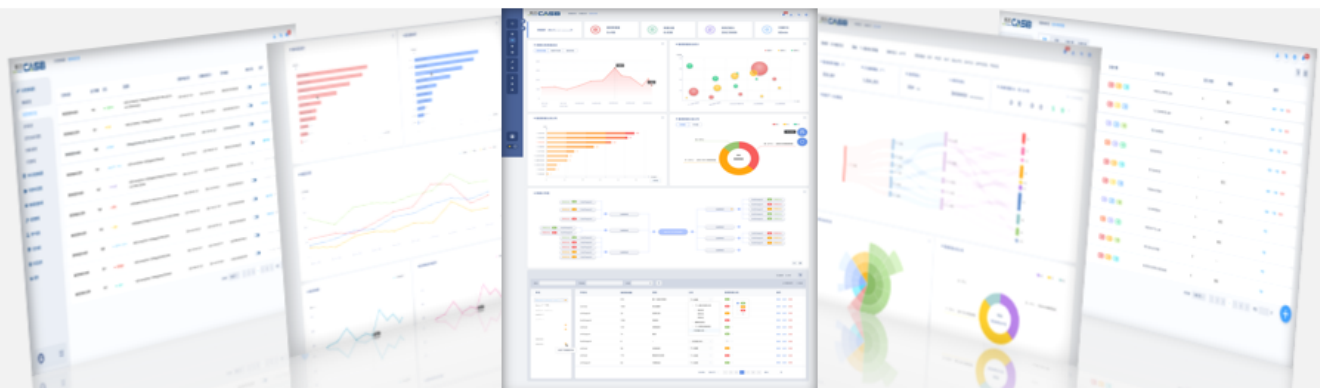
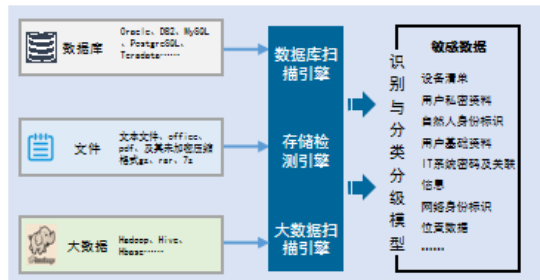
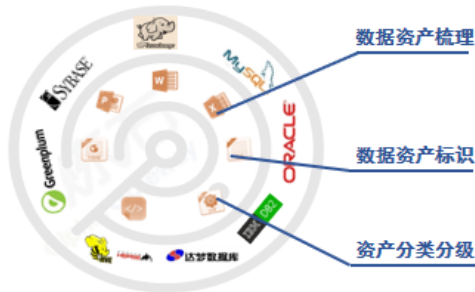
产品原理：免改造控制面“横向覆盖应用、纵向叠加安全”



实战防护产品：密码安全一体化，免改造打造数据防绕过保护



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

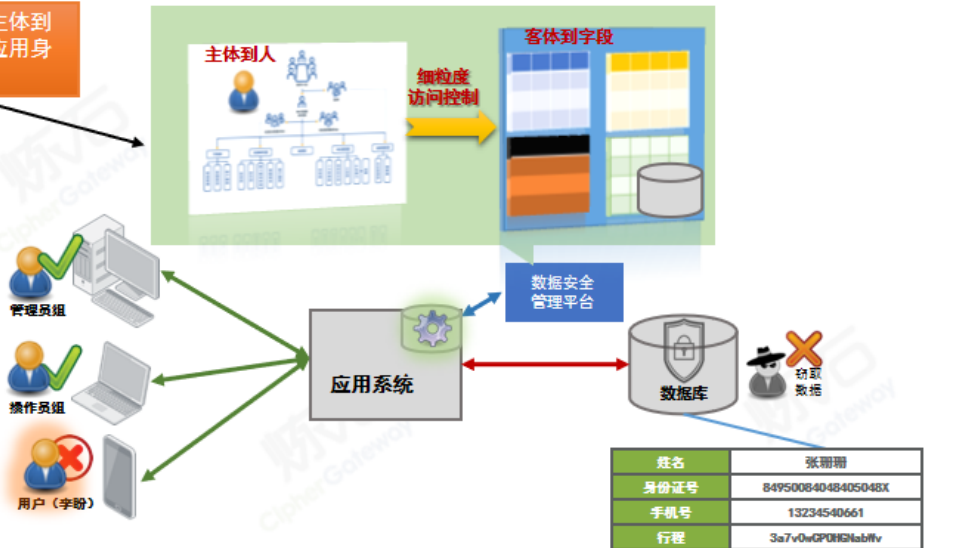
提供

易于实施的“主体到人”，支持与应用身份管理打通

姓名	张珊珊
身份证号	621087335677356125
手机号	13900334901
行程	Pvg-pok-pvg

姓名	张珊珊
身份证号	621087335677356125
手机号	13900334901
行程	Pvg-pok-pvg

姓名	张珊珊
身份证号	84950084048405048X
手机号	13234540661
行程	3a7v0wGP0HGhobllv



姓名	张珊珊
身份证号	84950084048405048X
手机号	13234540661
行程	3a7v0wGP0HGhobllv

- 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

事中检测：基于多控制面的数据风险识别

监测流量数据

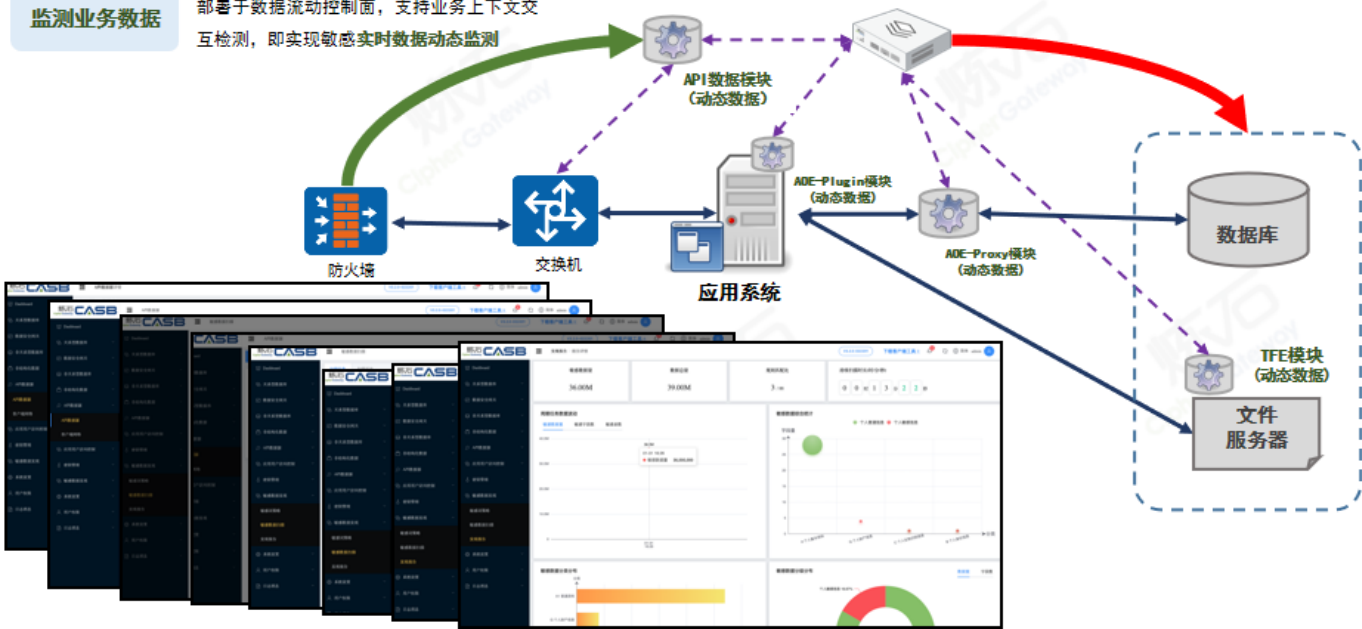
在支持SSL卸载情况下，敏感数据识别模块支持被动网络流量分析

监测业务数据

部署于数据流动控制面，支持业务上下文交互检测，即实现敏感实时数据动态监测

扫描静态数据

通过数据库或文件系统协议或接口主动扫描静态数据



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



数字/字符
型注入

搜索型
注入

数字/字符
型注入

数字/字符
型注入

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

规则ID	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，缺陷不允许。
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	把常量运算的条件，比如说WHERE FIB = 3 - 1，其中"3 - 1"是常量运算表达式。
.....	

示例

事中检测：业务人员风险操作监测

存储

使用

加工

传输

提供



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）

事后审计：可定责到人的访问审计追溯

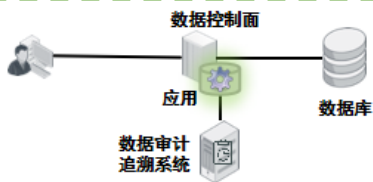
存储

使用

加工

传输

提供



记录所有访问敏感数据的行为

包括账号、时间、IP、会话、操作、对象、耗时、结果等内容，形成包含终端用户身份的SQL日志。用户可通过日志查询数据的访问情况，在事故发生后精确溯源

操作时间	操作者	行为	操作对象	操作对象ID	操作对象名称	操作对象所有者	状态	是否告警	告警类型	附件属性	客户端IP	日志签名
------	-----	----	------	--------	--------	---------	----	------	------	------	-------	------

操作时间	操作者	行为	操作对象	操作对象ID	操作对象名称	操作对象所有者	状态	是否告警	告警类型	附件属性	客户端IP	日志签名
2018-02-01 16:13:25	huhu	下载	附件	00_9	00_9	huhu	成功	否	否	279568	172.16.10.98	MEUC3QC7L...
2018-02-01 16:13:25	huhu	下载	附件	01_1	01_1	huhu	成功	否	否	213008	172.16.10.98	MEUC3ApAR...
2018-02-01 16:13:25	huhu	下载	附件	01_3	01_3	huhu	成功	否	否	95760	172.16.10.98	MEUC3GyGQ...
2018-02-01 16:13:24	huhu	下载	附件	01_13	01_13	huhu	成功	否	否	36134	172.16.10.98	MEUC3QYwefGQYAdwKq64d8RAw9OhaKUVwMT
2018-02-01 16:13:24	huhu	下载	附件	02_2	02_2	huhu	成功	否	否	376336	172.16.10.98	MEUC3QYw...
2018-02-01 16:13:24	huhu	下载	附件	04_4	04_4	huhu	成功	否	否	163344	172.16.10.98	MEUC389FG...

炼石数据安全分类分级服务

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。



序号	基本信息					数据是否共享	来源系统					对端系统名称					
	系统名称	部门	数据类型	对应数据	敏感级别		数据来源形式	系统来源单位/部门	来源系统名	来源数据类型	传输方式	对端系统名称	目标系统简介	对端系统单位/部门	数据开放形式	传输方式	备注
样例	旅游**	营销中心	用户位置数据	位置信息	4级	是	从其他数据采集	信息中心	精准营销	脱敏数据	FTP	旅游分析平台	地区人流量统计	旅游局	脱敏数据	TFTP	

业务数据流

业务数据流 转清单样例

炼石数据安全风险监测服务

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。

运营管理
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个子项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

网络安全、系统安全、大数据平台组件安全

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

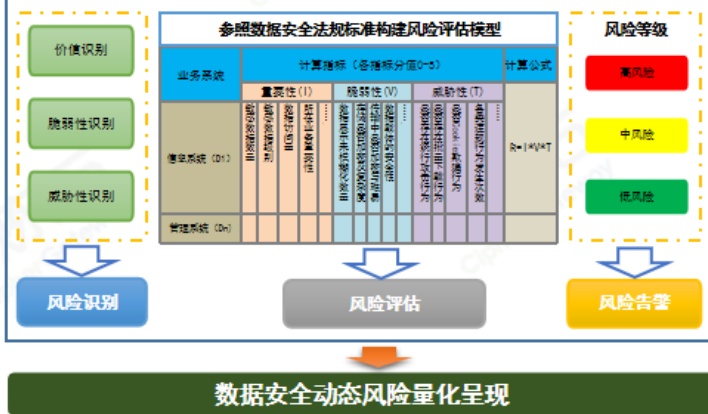
管理平台安全、4A及金库管控安全、安全事件管理、灾难恢复、日志审计、安全态势感知和监测预警

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。

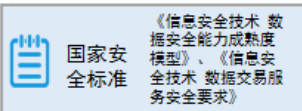
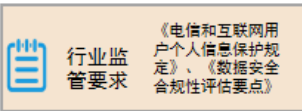
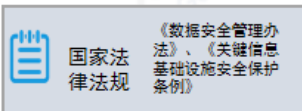
风险分析及量化模型



炼石数据安全合规检查服务

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



检查矩阵：

检查类

检查项

检查内容

检查依据等

应用矩阵：

适用对象

评判标准

测评模型

量化准则

0 合规自检

针对企业自身数据安全工作成效进行合规情况自查和效果验证。

0 考核抽检

针对上级主管部门对企业的数据安全工作要求落地情况的抽查与评估分析

安全风险量化呈现

数据流通保护实践

基于TEE技术的跨域数据管控

外发痛点：数据“可见即可转”，共享失控



数据已成为企业间可以交易的商品，但在交易后一直存在“数据失控”的问题困扰着数据的所有者：

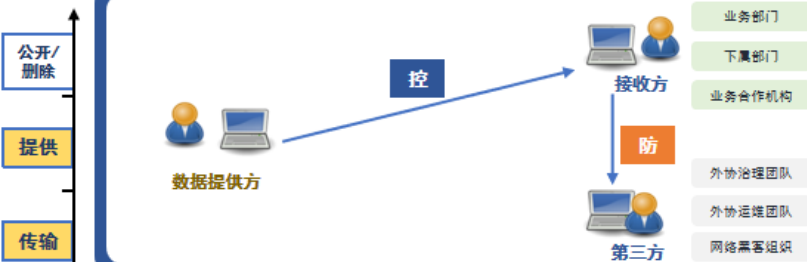
- 数据的接收方有没有对数据进行滥用？
- 对方有没有再次将数据外发给第三方？
- 这些数据在对方的有效期如何控制？



问题实质是，数据提供方仅赋予接收方数据使用权而非所有权，并且要按照约定来限制对方的使用范围。

现行做法是双方签订协议实现约束，但数据的所有权从技术上是失控的。数据不得不共享的前提下，必须从技术上实现对接收方使用数据的行为进行控制，防止数据滥用、防止数据泄露给第三方，维护数据提供方的利益。

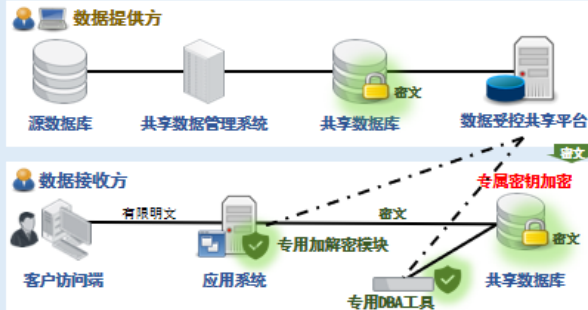
跨域数据：基于TEE的TDF技术，轻改造落地数据“可见不可转”



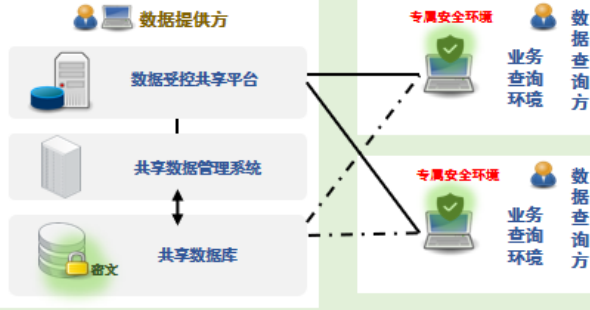
数据已成为企业间可以交易的商品，但交易后存在“数据失控”问题困扰着数据提供方：

- 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：实现数据可见不可转



I. 识别

P. 防护

D. 检测

R. 响应

R. 恢复

C. 反制

跨域管控：部署模式不改变原有数据共享流程



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。



案例—某国有骨干航空公司数据安全

项目背景介绍

客户行业：民航

项目名称：某民航系统数据加密升级改造

项目需求：

企业拥有大量旅客和员工的个人信息数据，受国外GDPR以及国内《网络安全法》、《密码法》等法律法规的合规要求，需要建设数据安全密码防护平台，采用密码技术保护个人信息以及企业敏感数据的安全。

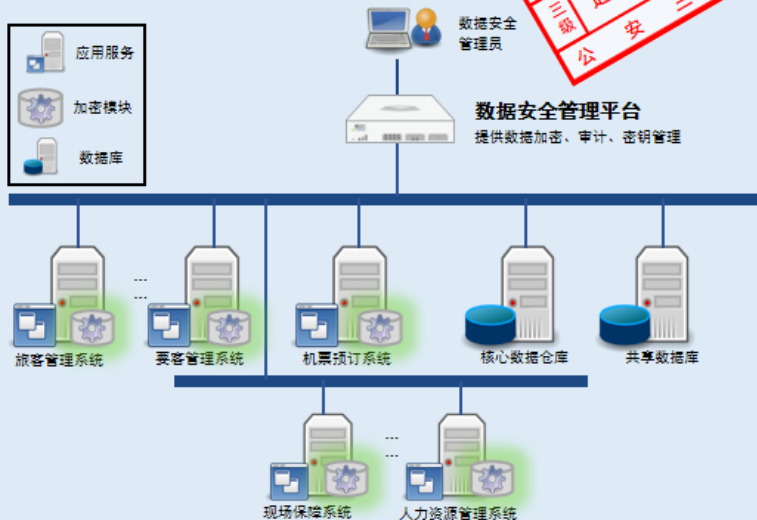
项目建设内容：

业务数据加密平台，用户访问控制，基于国密的字段级数据加密，以及面向用户授权的动态脱敏防护服务。

项目收益：

- 1、实现批量系统的应用数据加密需求，保护旅客隐私数据安全，提升系统安全水平。
- 2、满足国家关于个人隐私数据保护、商用密码信息系统密码应用规范要求。

部署和实施方案



案例-政府密评合规：深圳智慧党建系统应用与数据国密改造

项目背景介绍

客户行业：政府

项目名称：智慧党建国密整改

项目需求：

系统内含有重要敏感的党员信息及党组织信息。由于系统的重要敏感性，需要开展密评工作，测评中发现系统内大量敏感信息未采用国密标准方式进行完整性校验及加密存储保护，导致系统不满足密评合规的同时存在严重的信息泄露风险。

项目建设内容：

完成了11个数据库中近400个字段，1.5亿条数据的加密防护；

硬件产品需要托管到IDC机房，并通过了深圳信息安全测评中心的安全专项测评；

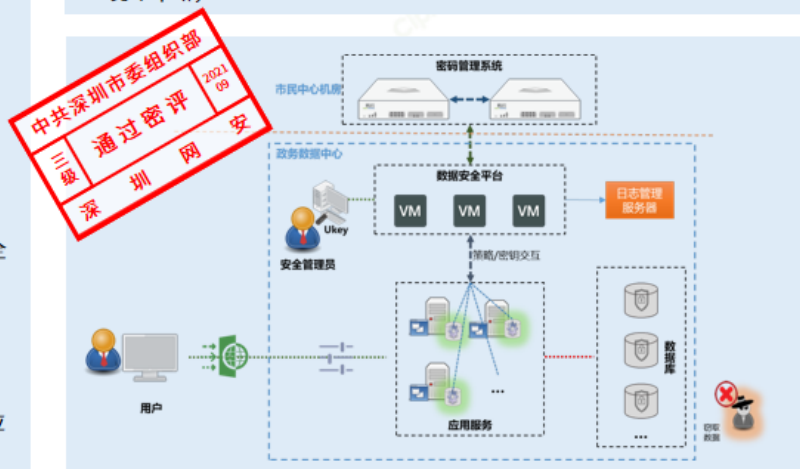
支持系统的微服务改造及分库分表等定制需求。

项目收益：

- 1、保护了超百万用户的党员、党组织等敏感信息。
- 2、满足国家关于政策合规、商用密码信息系统密码应用规范要求。

部署和实施方案

- ① 产品及方案顺利通过由深圳市网安计算机安全检测技术有限公司的密码应用安全性评估审查（密码测评）；
- ② 密钥管理系统及数据安全平台均采用高可用集群部署方式，通过keepalived及haproxy提供高业务量下的负载均衡，通过虚拟ip保障业务高可用，加密模块提供密钥及策略的安全缓存机制，保证在平台断连的情况下业务不中断；



案例-国家重大活动关键应用：2022某国际综合体育赛事数据加密

客户需求

某国际综合体育赛事组委会建立的招聘应用系统，是面向全球招聘工作人员的网站，其中涉及到应聘者的**个人信息**，比如手机号、身份证号、护照信息、宗教信仰等。随着GDPR和中国《网络安全法》实施，无论从风险驱动还是合规层面，保护这些个人信息迫在眉睫。

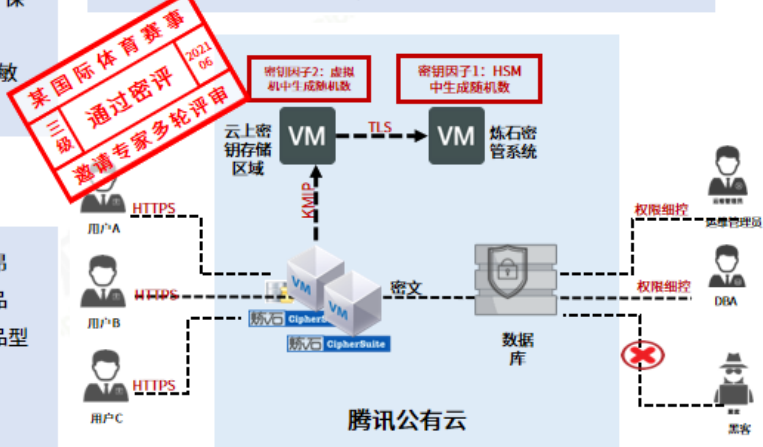
经过分析，总结出应聘者相关的14项个人信息是关键、敏感信息，需要对这些**敏感字段加密保护**，并选用**国密算法**。

客户痛点

- 应聘系统为国外开发，对应用系统进行二次开发成本高昂
- 系统部署在腾讯公有云，无法部署加密机等国密硬件产品
- 需选择软件形态的解决方案，同时具备国密局认可的产品型号证书
- 密钥需要安全保护，由组委会掌控
- 网站访问量高，加密执行不能影响系统的正常使用

解决方案

- ① 将数据安全模块部署在应用系统内，配置加解密规则
- ② 用独立KMS管理根密钥，根密钥由组委会掌控。
- ③ 应用服务在向数据库保存个人信息之前，通过模块对敏感字段进行加密。在显示应聘者的个人敏感信息时，应用服务将密文读出并通过模块进行解密，再将明文信息返回给前台展示



案例-政府关键应用：海量敏感个人信息保护

项目背景介绍

客户行业：政府

项目名称：某直辖市XX码海量敏感个人信息保护

项目需求：

某直辖市XX码系统包含海量公民隐私信息，蕴藏巨大价值，是外敌对势力、灰黑产等攻击的重点目标。《密码法》《GB/T 38961-2020个人健康信息码参考模型》等法律法规要求，采用符合国家密码管理要求的算法进行加密保护。在抗疫持久战局势下，健康码亟待实施基于商用密码的实战化数据安全防护

项目建设内容：

1. 涉及某直辖市3000万市民在10个应用系统中15个字段的、1.4亿条数据进行加解密实施；
2. 方案调研和设计花费3天，分2天分批上线（实际为2个4小时，实施窗口期只有0点-4点）。

项目收益：

1. 让XX码业务正常运转和安全防护二者兼得，保护了3000万人民的隐私信息；
2. 通过密评方案评估，其创新技术示范可复制到更广泛场景。

部署和实施方案



案例-金融关键应用：某交易所重要数据保护

项目背景介绍

客户行业：金融

项目名称：某大型证券交易所数据安全项目

项目需求：

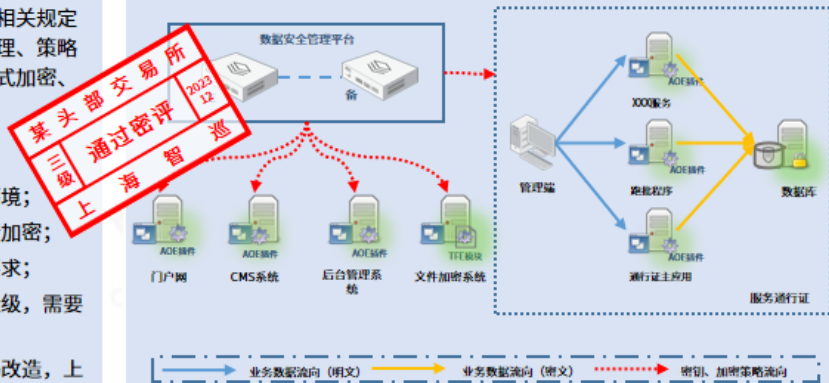
行情经营、网站等相关的多个系统中均存在大量的会员相关信息，如会员账号、股东账号、个人邮箱、真实姓名等敏感数据，数据需要在日常业务中高速流转。依据行业及国家相关规定，需要对敏感数据进行保护。需要实现密钥的统一管理、策略的统一管理、加解密元数据的统一管理，实现“分布式加密、集中式管控”的保护体系。

项目实施痛点：

- 生产应用使用信创环境，需要完全适配当前信创环境；
- 需要使用国密算法，对系统中存放的敏感数据进行加密；
- 需要通过国家密码管理部门核准，符合密评审核要求；
- 应用存在批量数据导入场景，单次导入数据千万量级，需要在执行批量导入时加密数据不影响系统使用；
- 新增解决方案在部署过程中无需应用系统进行代码改造，上线变更需要操作快，周期短；

项目建设方案

在数据中心机房部署两套数据安全平台，平台旁路部署，使用高可用部署模式。在应用侧部署免改造加密插件实现对业务系统中结构化(AOE 插件)和非结构化(TFE 插件)数据的存储加密，提供有效且易于实施的数据安全保护。



炼石免改造数据安全

THANKS



www.ciphergateway.com



010-88459460



sales@ciphergateway.com