



中华人民共和国密码行业标准

GM/T 0066—2019

商用密码产品生产和保障能力建设 实施指南

Implementation guide to capability construction criteria of production and
guarantee for commercial cryptographic products

2019-07-12 发布

2019-07-12 实施

国家密码管理局 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 实施概述	1
4.1 评估内容	1
4.2 评估方式	1
4.3 评估原则	2
5 实施指南	2
5.1 基本项	2
5.1.1 法人资格	2
5.1.2 主要技术人员	2
5.1.3 产品研发	2
5.1.4 行业管理遵从	2
5.2 声明项	2
5.2.1 关键人员信息	2
5.2.2 单位性质	2
5.2.3 数据管理	2
5.3 评估项	3
5.3.1 生产能力	3
5.3.2 质量保障能力	5
5.3.3 安全保障能力	6
5.3.4 服务保障能力	7
6 评估程序	7
6.1 评估要求	7
6.2 评估流程	8
6.3 实施评估	9
6.3.1 材料审查	9
6.3.2 前置评估	9
6.3.3 现场审核	9
6.3.4 专家评估	10
6.3.5 评估结果	10
7 评估报告	10
7.1 报告内容	10
7.2 报告形式	10

7.3	报告要求	10
7.3.1	评估时间	10
7.3.2	评估地点	10
7.3.3	评估组和评估监督人员	10
7.3.4	生产单位基本信息	10
7.3.5	申请产品基本信息	10
7.3.6	评估材料是否齐全	10
7.3.7	基本项是否符合要求	10
7.3.8	现场审查	11
7.3.9	声明项说明	11
7.3.10	评估项说明	11
7.3.11	评估结论	11
7.4	报告归档	11
8	实施要点说明	11
8.1	评估单位	11
8.1.1	评估过程	11
8.1.2	专家评分	11
8.1.3	商用密码产品不同等级的许可要求	11
8.1.4	特殊申请要求说明	12
8.2	生产单位	13
8.2.1	能力建设	13
8.2.2	自评估	13
附录 A (规范性附录)	商用密码产品生产和保障能力评估配套表格	14
附录 B (规范性附录)	商用密码产品生产和保障能力评估报告	26
附录 C (资料性附录)	审核方法	27
附录 D (资料性附录)	归档材料清单	28
附录 E (资料性附录)	重要领域产品使用要求	29
参考文献		30

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：兴唐通信科技有限公司、北京中电华大电子设计有限责任公司、格尔软件股份有限公司、国家密码管理局商用密码检测中心、北京三未信安科技发展有限公司、天地融科技股份有限公司、成都卫士通信息产业股份有限公司、北京市密码管理局、上海市密码管理局、广东省密码管理局。

本标准主要起草人：赵闪、叶枫、周建锁、罗鹏、冯育晖、韩小平、杨耀华、高志权、熊云、李立勋、马飞、郑强、李明、曲志华、杨阳。

引 言

密码是网络和信息安全的核心技术和基础支撑,是保障国家安全、推动经济发展和维护公众利益的战略性资源。商用密码产品是密码技术的实现载体,为应用提供机密性、完整性、不可否认性等安全保障。国家对销售或者在经营活动中使用的商用密码产品实施许可。

根据《商用密码管理条例》的相关要求,商用密码产品生产单位(以下简称生产单位)必须具备独立的法人资格,具有与开发、生产商用密码产品相适应的技术力量和场所,具有确保商用密码产品质量的设备、生产工艺和质量保证体系,满足法律、行政法规规定的其他条件。

本标准是 GM/T 0065—2019 商用密码产品生产和保障能力建设规范的具体实施指南。

商用密码产品生产和保障能力建设 实施指南

1 范围

本标准规定了实施商用密码产品生产和保障能力评估的方法、程序、报告和要点说明。

本标准适用于对生产单位的生产能力、质量保障能力、安全保障能力和服务保障能力进行建设指导。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GM/T 0008—2012 安全芯片密码检测准则

GM/T 0028—2014 密码模块安全技术要求

GM/T 0065—2019 商用密码产品生产和保障能力建设规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 及 GM/T 0065—2019 界定的以及下列术语和定义适用于本文件。

3.1

形式审查 formal examination

审查生产单位提交的申请材料在形式上的合规性、完整性和有效性。

3.2

实质审查 substantive examination

在形式审查的基础上,审查生产单位是否具备主体资格条件,所申请的事项是否真实,提交的文件、证件是否真实、有效、完整、合规,是否符合国家法律法规的规定。包括书面审查和现场审核等方式。

4 实施概述

4.1 评估内容

评估内容包括基本项、声明项和评估项等评估要素。

基本项包括生产单位法人资格项、主要技术人员项、产品研发项、行业管理遵从项等内容。

声明项包括生产单位关键人员信息、单位性质、数据管理等内容。

评估项包括生产单位生产能力、质量保障能力、安全保障能力和服务保障能力等内容。

4.2 评估方式

对商用密码产品生产和保障能力进行评估采用单位自证和专家评分相结合的方式,质量保障、安全

保障以及服务保障能力应为单位的自证项,由生产单位提供商用密码产品生产和保障能力的证明;结合生产单位的基本项、声明项,专家组根据评估项的评估要素进行评分判定。

4.3 评估原则

对商用密码产品生产和保障能力进行评估应基于生产单位提交的申请材料采用“材料审查”与“现场审查”相结合、“前置评估”与“专家评估”相结合等方式,遵循“定量评估”与“定性判定”的评估原则以确保申请材料的真实性、一致性和符合性,本着公平公正、保密性、独立性和基于证据的基本原则,对生产单位的生产能力、质量保障能力、安全保障能力和服务保障能力等进行评估。

5 实施指南

5.1 基本项

5.1.1 法人资格

生产单位为中国境内注册的独立法人,应出具生产单位营业执照注册号;应出具法定代表人有效身份证件的名称和号码。

5.1.2 主要技术人员

生产单位从事密码产品设计、实现、检测或测试、技术支持等工作的主要技术人员应不少于 15 人,并提供相关信息,否则终止评估流程。相关信息包括但不限于国籍、学历、工作简历、专业特长及现从事工作等。

5.1.3 产品研发

生产单位应承诺所研发产品及产品涉及的密码核心技术具有自主知识产权,应拥有专利、软件著作权、集成电路版图布图登记等;应承诺申请评估材料对应产品不包含其他任何组织或单位的知识产权或已通过合法方式取得。

5.1.4 行业管理遵从

- a) 生产单位应签署承诺文件,应做好产品销售记录并如实申报产品年度销售情况,承诺提供源代码,将源代码提交经密码管理部门认可的检测机构;
- b) 生产单位应履行上述承诺,否则终止评估流程。

5.2 声明项

5.2.1 关键人员信息

生产单位应提供关键人员的证件名称及号码、国籍、教育背景和从业经历的详细介绍。

5.2.2 单位性质

生产单位应提供单位性质的声明,按照合法营业执照的内容如实提供,包括注册资本结构、注册资金规模、投资人名称、投资比例等。如有自然人,应说明自然人人数、姓名、国籍;如有外资成分,说明外资比例及外资参与公司经营管理的状况。

5.2.3 数据管理

生产单位应提供商用密码产品研发、生产和保障数据中心所在地的声明,说明数据中心所在地、数

据流转是否会涉及出境等情况。

5.3 评估项

5.3.1 生产能力

5.3.1.1 技术力量

5.3.1.1.1 人力资源

- a) 生产单位应设置研发、生产和管理关键岗位；
- b) 关键岗位宜由经验丰富、专业技术深厚的资深人员担任；
- c) 生产单位的岗位设置和人员资格应满足人力资源设置，评判标准包括岗位设置是否齐备合理、任职资格是否清晰等。

5.3.1.1.2 主要技术团队

- a) 应核实生产单位中从事密码技术设计、实现、检测或测试和技术支持人员的数量，及本科以上人员占技术团队的比例等；
- b) 应考核核心技术负责人的密码专业技术能力，评判标准至少包括从业经历、学历职称、研究成果及获奖情况等。

5.3.1.1.3 技术积累及优势

- a) 生产单位所申请的产品应符合生产单位的主营业务方向；
- b) 生产单位在产品生产过程中应有效利用自身的科研资源，保证产品具备较高的技术水平；
- c) 生产单位应具备相关科研成果和技术储备。生产单位应有与所申请产品相关领域的专业技术研究成果且该成果得到过实际应用，且近5年来生产单位应开展过与所申请产品类似项目的科研并有技术储备；
- d) 生产单位的专业技术水平应满足所申请产品的需求，宜达到国内先进水平。

5.3.1.1.4 技术创新

- a) 生产单位应具备授权专利、软件著作权、集成电路版图布图登记等；
- b) 生产单位应明确申请产品是否经专家鉴定认为填补国内或国际行业应用空白；
- c) 生产单位应明确申请产品是否具备高性价比，是否在成本、功能、性能、可靠性、市场应用等方面具有良好的市场发展空间。

5.3.1.1.5 研发工具和设备

- a) 生产单位应具备满足研发需求的工具和设备；
- b) 生产单位应具备满足申请产品研发相关的主要研发工具，如工作站、专用软件、开发板、仿真器、示波器、逻辑分析仪等。

5.3.1.1.6 试验测试条件

- a) 生产单位应具有较完善的密码产品功能、性能、稳定性、可靠性、环境适应性(如电磁兼容)等试验测试条件；
- b) 密码产品环境适应性检测应能保证密码产品在生产、运输、贮存、使用等环境下功能正常；
- c) 密码产品可靠性检测应能保证密码产品在产品生命周期内无故障的实现功能。

5.3.1.2 生产管理

5.3.1.2.1 岗位设置

生产单位应设置生产主管、仓储管理等相关的岗位,并确保由经验丰富、认真负责的资深专业人士担任相关职务。

5.3.1.2.2 制度保障

生产单位应制定相应生产管理规章制度和仓储管理制度,并建立生产记录档案且确保生产记录可查询和追溯。

5.3.1.2.3 管理系统

- a) 生产单位应建立完善的产品出入库记录档案,并确保产品出入库记录可查询和追溯;
- b) 生产单位应建立产品数量管理要求,并确保数量管理的准确性。

5.3.1.2.4 供应管理

- a) 生产单位应考核供应商或外协单位是否具备相应的资质和技术能力,应提供供应商或外协单位的资质和能力证明材料;
- b) 生产单位应对供应商供货环节和外协加工环节具备控制和监管措施;
- c) 生产单位应设立专职负责供应商及外协单位质量监视、测量和验收及提供外加工产品的质量
标准,保证外协加工环节对产品质量无影响;
- d) 生产单位应与供应商签订质量保证协议并定期进行质量审查,对外包人员、过程 and 外包工作有明确管理规定。

5.3.1.3 生产条件

5.3.1.3.1 生产场所

- a) 生产单位应具备生产场所土地及房屋使用权,生产设施和仓储场所应满足需求;
- b) 对自有生产场所的情况,应核对生产场所的产权证明文件或租赁合同,以确认生产单位具备固定的生产场所,并具备满足生产基本需求的基础设施(如水、气、电供应设施等)和支持性服务设施(如运输、通讯、信息化手段等),以保证生产设施安全可靠运行;
- c) 生产单位如采用外协加工的方式,应具备相应的仓储场所,仓储场所应满足产品仓储需求,保证产品免受各种物理损伤;
- d) 可对外协加工的生产场所进行评估。

5.3.1.3.2 生产设备

- a) 生产单位应具备满足生产要求的生产设备和检测设备;
- b) 生产单位进行商用密码产品生产所需的生产辅助工具、加工、试验、检测设备及计量器具等设备应满足需要;
- c) 生产单位如采用外采或外协方式,则外采或外协单位应满足本条中 a)、b)项要求。

5.3.1.4 生产工艺与流程

5.3.1.4.1 生产技术管理

生产单位应具有管理规范 and 齐全的生产技术文件,至少包括生产清单、物料清单、检验流程和报告

文件。

5.3.1.4.2 批量生产和检测能力

生产单位应具备批量生产和检测能力,宜具备自动化生产线及相应的产品检测机制,以保障产能充足、产品质量稳定;应具备规定的检验、试验和计量设备,以满足与生产规模相适应的需要。

5.3.2 质量保障能力

5.3.2.1 制度保障

- a) 生产单位应建立质量管理体系,明确质量目标并落实实施;
- b) 生产单位应保证商用密码产品的质量,设立质量管理岗位并明确岗位职责,在商用密码产品生产过程中应建立各阶段的质量目标并由生产单位高层负责实施;
- c) 生产单位应建立服务质量保障体系,明确对服务质量的标准要求,对服务质量进行监督并评估,并提供必要的技术保障服务。

5.3.2.2 开发过程质量管理

5.3.2.2.1 开发与测试体系

- a) 生产单位应建立完备的开发与测试体系,以保证产品的质量;
- b) 开发体系宜包括系统集成设计规范、系统集成管理规范、编码规范、设计规范、开发管理规范、变更管理规范等;
- c) 测试体系宜包括单元测试、集成测试、系统测试和验收测试等。

5.3.2.2.2 研发过程管理

- a) 生产单位应对研发过程进行管理和控制;
- b) 生产单位研发过程应有专人跟踪并组织协调,整个过程应有明确的阶段划分和过程管理;
- c) 生产单位应定期对项目进行评审和审核,应对变更进行管控;
- d) 生产单位应有详尽的技术设计方案,应对技术性文档进行归档;
- e) 生产单位应对用于检验、量测与判定产品质量的测试设备进行管制、定期校正与维护,维持测试设备的准确性能。

5.3.2.2.3 版本管理

- a) 生产单位应制定配置管理制度;
- b) 生产单位应设置配置管理人员;
- c) 生产单位宜使用配置管理工具和方法。

5.3.2.2.4 质量问题管理

- a) 生产单位应对质量问题具有管理和控制措施,并就质量问题的解决进行跟踪管理;
- b) 生产单位应建立质量问题处理制度和流程,具备质量问题跟踪和统计的能力,对质量问题处理的时效性进行要求,并对客户进行满意度调查。

5.3.2.3 持续改进产品质量措施

- a) 生产单位应具有合理的持续改进产品质量的措施;
- b) 生产单位应对产品质量进行持续跟踪监控,收集产品质量改进的信息,并据此制定产品质量改

进计划。

5.3.2.4 质量体系认证

应对生产单位的第三方质量体系认证进行核实,对于已获得相应认证并在有效期之内的生产单位,可对质量保障能力评估得分,如生产单位具有 ISO 9001 质量体系认证或 CMMI 3 级及以上能力成熟度认证。

5.3.3 安全保障能力

5.3.3.1 组织保障

- a) 生产单位应明确安全的重要性,建立组织范围内的安全目标;
- b) 应由高层管理人员承诺保证安全研发和生产;
- c) 生产单位应由专人或部门(组织)负责安全;
- d) 生产单位应定期进行组织内部安全管理制度的审核和评审,确保安全管理体的适宜性和有效性;
- e) 生产单位应建立组织预防、处理安全事件机制;
- f) 生产单位应与员工签署正规的劳动合同并对员工进行安全培训;
- g) 生产单位应与相关岗位员工签署保密合同或合同中包含着安全条款并对相关岗位员工进行商用密码条例的培训;
- h) 生产单位应对离职的单位员工设置信息资产归还和访问权限撤销的规定;
- i) 生产单位应对纠正和危害安全的行为进行适当的鼓励和惩罚。

5.3.3.2 安全管理

- a) 生产单位应建立安全生产规章制度并贯彻执行,应了解国家和行业的安全生产规定和标准,制定安全生产责任制和安全操作流程。
- b) 生产单位应划分物理安全区域并任命相应的负责人,重要区域应安装门禁系统并对访问进行记录且记录可查询,监控的内容记录至少保存 30 天以上。重要资产进出单位或重要区域应实行审批机制,重要区域设置温湿度要求并配备不间断电源,由安全负责人定期对机房防火、防雷、防漏、防尘等规程进行检查和记录。
- c) 生产单位应具备计算机软件防护措施和网络防护措施。重要信息资产应有专人维护,有远程及移动办公安全管理制度或条款,应识别计算机资产脆弱性和潜在威胁,建立适应组织的信息安全策略,保证信息存储、交换和销毁过程中的信息安全,且应具备应急灾备计划。
- d) 生产单位应对组织访问机制有控制。重要区域应有识别并重点保护,通过网络接入单位内网应有访问控制,员工对信息访问应具有访问策略控制,应安全传输、接收和处理关键数据,及时删除存储介质上的数据或销毁存储介质,并详细记录存放信息。
- e) 生产单位应具备移动存储介质的安全管理制度。应建立对存储介质申请、使用、更换、维修及报废的管理制度和策略,保存对关键存储介质定期检查的记录,执行写操作以覆盖旧内容并确保不可恢复,对不再利用的介质应采用毁损的方式进行物理销毁并确保存储内容不可恢复。
- f) 生产单位应设立开发安全制度或条款。应具备项目开发安全风险识别和控制措施,配置管理或权限控制措施,外协/外包如涉及商业秘密应签署保密协议,且外协/外包不包含密钥安装及关键参数配置。
- g) 生产单位应具备风险预警及应急处置措施,制定与本单位采用的资产管理分类方案一致的信

息标识和处理程序,并依据实施。

- h) 生产单位应对用户活动、意外和信息安全事件日志、系统管理员和系统操作者的活动进行记录并保存,保护日志设施和日志信息免受破坏和未授权的访问,对错误日志进行分析并采取适当的措施。
- i) 生产单位应确保与信息系统有关的安全弱点和安全事件的内部沟通,并及时采取相应措施,使用持续有效的方法管理信息安全事故。
- j) 生产单位应防止业务活动中断,保护关键业务流程不受信息系统重大失效或自然灾害影响,确保及时恢复。

5.3.3.3 信息安全体系认证

应对生产单位的信息安全体系 ISO 27001 认证进行核实,对于已获得相应认证并在有效期之内的生产单位,安全保障能力评估项可以得分。

5.3.4 服务保障能力

5.3.4.1 制度保障

生产单位应设置完善的服务保障制度,根据服务管理的策划实施服务管理并提供服务、监督、测量和评审并持续改进。

5.3.4.2 应急响应能力

- a) 生产单位应建立应急响应机制并统筹规划、协调管理;
- b) 生产单位应具有解决突发问题的能力,通过问题原因的识别和分析尽快恢复约定的服务要求,最小化对业务的影响;
- c) 生产单位应在解决过程中及时向用户报告进展和最新状态。

5.3.4.3 服务响应方式

- a) 生产单位应建立完善的服务网络,结合产品应用情况提供符合使用单位需求的产品服务;
- b) 生产单位应明确产品技术服务承诺内容和可操作的服务方案;
- c) 生产单位应建立如呼叫中心、网络、当地客户服务部门等多种方式的官方受理渠道,保证客户可反馈意见和问题;
- d) 生产单位应记录用户来函反映及投诉问题,应明确问题处理期限,并将相应处理的结果形成报告;
- e) 生产单位应建立客户档案;
- f) 生产单位应对客户进行服务质量满意度调查。

5.3.4.4 服务管理体系认证

应对生产单位的信息技术服务管理体系 ISO 20000 认证进行核实,对于已获得相应认证并在有效期之内的生产单位,可以对服务保障能力项得分。

6 评估程序

6.1 评估要求

按照 GM/T 0065—2019 及 4.3 的要求,基于生产单位提交的申请资料进行评估。对申请资料进行

形式审查和实质审查,并在必要时启动现场审核。

6.2 评估流程

评估流程如图 1 所示。

- a) 对申请材料进行形式审查,通过后进入实质审查阶段;
- b) 前置评估阶段主要对申请材料中的基本项、声明项等内容进行审核,不符合基本项、不提供声明项或提供材料不完整时,终止评估流程;
- c) 根据前置评估情况,判断是否有必要进行现场审核,现场审核阶段主要核查生产单位的实际情况与申请材料的一致性;
- d) 评估组专家成员应对评估项的各项指标进行评分,并给出评估结果;
- e) 完成审核评估后应由评估组出具评估报告。

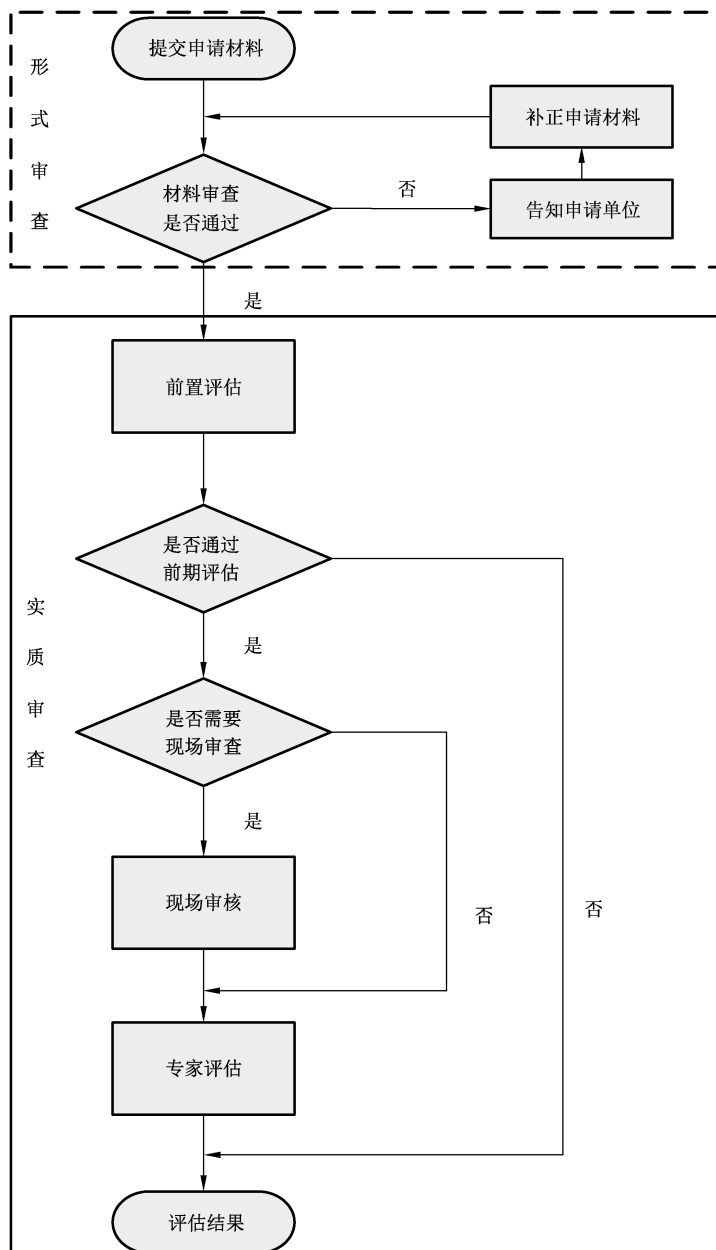


图 1 商用密码产品生产和保障能力评估流程

6.3 实施评估

6.3.1 材料审查

收到生产单位提交的评估申请材料后,首先对申请材料进行形式审查。

如果未通过形式审查,生产单位收到通知后,补正并重新提交申请材料,再次进行形式审查。

6.3.2 前置评估

6.3.2.1 评估启动

应确定评估组长,及 2 名以上专家组成评估组,评估组人数应不少于 3 人,评估组,成员应对评估对象、评估内容进行保密承诺。

应设置独立的评估监督人员,对评估工作实施的规范性、公正性进行监督。

应确定评估的目的、范围、依据和方式。

应编制评估项评分表,包括基本项、声明项、评估项,评估项为评分,见附录 A。

6.3.2.2 前置评估

评估组对申请材料进行前置评估,主要是对基本项、声明项等内容和证明文件进行审核。

基本项的所有要求必须满足,并审核相关材料的真实性和符合性。如存在不符合项,或存在与事实不符的情况,则终止评估流程,并将不符合情况记录到评估结果。

声明项不作为判定和评估的依据,但要保证相关材料的真实性。如缺少必要的声明项,或存在与事实不符的情况,则终止评估流程,并将不符合情况记录到评估结果。

6.3.3 现场审核

6.3.3.1 审核判断

评估组应根据生产单位的具体情况进行判断是否需要现场审核。如申请材料真实性缺少佐证、申请条件符合性差、生产单位曾受过相关行政处罚等,应进行现场审核。

评估组应对生产单位不同类别首款产品进行现场审核。

6.3.3.2 审核通知

如需对生产单位进行现场审核,应与生产单位就现场审核实施进行初步联系。初步联系至少包括以下工作:

- a) 与生产单位的代表建立沟通渠道;
- b) 提供有关审核目标、范围、依据和方式等信息;
- c) 请求有权使用用于审核评估的相关文件和记录;
- d) 确定与生产单位的活动和产品相关的应适用法律法规的要求、第三方要求、合同要求和其他要求;
- e) 对审核日程做出安排;
- f) 确定对特定区域的访问及安全控制。

6.3.3.3 审核方法

现场审核应核查申请材料的真实性和有效性。审核过程中,应通过适当的抽样收集并验证与审核目标、范围和 GM/T 0065—2019 相关的信息,包括组织职能、生产及研发的活动和过程等有关信息。

应以能够验证的信息作为审核依据,对发现的审核证据予以记录。

审核过程中采用的方法参见附录 C。

6.3.4 专家评估

评估组应根据评估项建立评分表,对生产单位产品生产和保障能力进行核实并评分。

评估组专家应独立完成评分。

6.3.5 评估结果

评估结果以评估报告方式提出,评估组应提供统一的评估结论。

7 评估报告

7.1 报告内容

报告内容应完整、真实、客观,明确生产单位基本信息、申请产品基本信息、评估组人员、评估监督人员、评估时间、评估材料是否齐全、基本项是否符合要求、是否会现场审查、声明项和评估项说明以及评估结论。

7.2 报告形式

评估报告形式为表格,见附录 B。

7.3 报告要求

7.3.1 评估时间

评估报告中应明确启动评估工作的时间,格式为“××××年××月××日”。

7.3.2 评估地点

评估报告中明确评估地点。

7.3.3 评估组和评估监督人员

评估报告中明确评估组和评估监督人员姓名。

7.3.4 生产单位基本信息

评估报告中应明确生产单位名称、单位类型以及所属省(区、市),其中生产单位名称和单位类型应按照其营业执照填写。

7.3.5 申请产品基本信息

评估报告中应明确生产单位申请的许可产品名称和类型。

7.3.6 评估材料是否齐全

应明确评估生产单位提交的材料是否齐全,明确方式为选择“是”或“否”。

7.3.7 基本项是否符合要求

应参照 5.1 的描述,明确生产单位的基本项是否符合要求,明确方式为选择“是”或“否”。

7.3.8 现场审查

应明确是否现场审查,明确方式为选择“是”或“否”。

7.3.9 声明项说明

应参照 5.2 描述,明确生产单位的关键人员、企业性质和数据管理信息。

- a) 应明确生产单位的关键人员是否持有外国国籍、绿卡和港澳台籍,明确方式为填写“是”或“否”。
- b) 若生产单位为企业,应明确企业资本结构,如企业性质为合资,应注明企业外资和内资比例。
- c) 应明确注明生产单位的数据中心所在地,以及数据流转是否涉及出境,如有出境,应明确数据流转环节和流转地。

7.3.10 评估项说明

应参照 5.3 和 8.1.2 的描述,明确生产单位生产能力、质量保障能力、安全保障能力和服务保障能力的得分。

7.3.11 评估结论

应参照 8.1.3 的描述,对生产单位是否具备申请产品类型和安全级别相适应的生产和保障能力给出结论,并明确给出结论的时间。

7.4 报告归档

应做好评估材料的归档,归档材料包括产品品种和型号申请材料、评估报告、评估记录,参见附录 D。

评估记录包括评估成员独立的评分表、监督人员记录等。

8 实施要点说明

8.1 评估单位

8.1.1 评估过程

应依据第 6 章规定的评估程序开展评估工作,包括材料审查、前置评估、现场审核和专家评估。

应根据生产单位背景、申请许可的产品类型和申请材料确定是否需要进行现场审核。

8.1.2 专家评分

专家评估以评分方式进行,评分结果包括单项分和综合分。

单项分包括生产能力、质量保障能力、安全保障能力和服务保障能力等四个单项的得分。多名专家评分结果中总分的平均值作为综合分,多名专家评分结果中单项得分的平均值作为单项得分。

8.1.3 商用密码产品不同等级的许可要求

商用密码产品生产及保障能力应与商用密码产品安全等级相适应。

与 GM/T 0008 规定的不同安全等级密码芯片相适应的单项分和综合分要求见表 1。

表 1 不同等级的密码芯片所需要的生产和保障能力要求

评估项	得分	密码芯片		
		1 级	2 级	3 级
生产能力	A1	≥60%	≥70%	≥80%
质量保障	A2	≥80%		
安全保障	A3	≥60%	≥70%	≥80%
服务保障	A4	≥70%		
综合得分	A	≥70%	≥80%	≥90%

与 GM/T 0028 规定的不同安全等级的密码模块相适应的单项分和综合分要求见表 2。

表 2 不同等级的密码模块所需要的生产和保障能力要求

评估项	得分	密码模块			
		1 级	2 级	3 级	4 级
生产能力	B1	≥50%	≥60%	≥70%	≥80%
质量保障	B2	≥80%			
安全保障	B3	≥50%	≥60%	≥70%	≥80%
服务保障	B4	≥70%			
综合分	B	≥60%	≥70%	≥80%	≥90%

8.1.4 特殊申请要求说明

对于生产单位、研制单位、加工单位存在不是同一个单位(企业、事业单位)的情况如表 3 所示。

表 3 生产单位与研制和生产单位关系

情况	生产单位	研制单位	加工单位
1	A	A	A
2	A	A	B
3	A	B(境内)	A 或 B 或其他
4	A	B(境外)	A 或 B 或其他

- a) 对于情况 1、情况 2、情况 3 和情况 4,生产单位 A 必须是在境内注册的独立法人单位,且生产单位 A 应具有 GM/T 0065—2019 规定的商用密码产品生产和保障能力;
- b) 对于情况 2,生产单位 A 自行研制商用密码产品,生产单位 B 为生产单位 A 的生产外包供应商,生产单位 A 应具有对生产单位 B 的有效管理能力;
- c) 对于情况 3,生产单位 A 自行或外包生产商用密码产品,研制单位 B 为生产单位 A 的产品委外研制的境内合作伙伴,此种情况下,生产单位 A 和研制单位 B 均应具备符合 GM/T 0065—2019 要求的生产和保障能力;
- d) 对于情况 4,生产单位 A 为自行或外包生产商用密码产品,研制单位 B 为生产单位 A 的产品

委外研制的境外合作伙伴,此种情况下,生产单位 A 应具备符合 GM/T 0065—2019 要求的生产和保障能力。

8.2 生产单位

8.2.1 能力建设

生产单位在实施生产与保障能力建设时,应参照本标准要求。

8.2.2 自评估

生产单位应依据 GM/T 0065—2019 进行自评估,根据自评估结果进行持续改进。

附 录 A
(规范性附录)

商用密码产品生产和保障能力评估配套表格

A.1 商用密码产品生产和保障能力评分表

商用密码产品生产和保障能力评分表如表 A.1 所示：

- a) 本表涉及的商用密码产品生产和保障能力评估体系包含 3 个分类, 11 个指标(含 4 个关键指标), 13 个指标分项。评估采用关键指标不达标一项否决和评分项打分相结合的方式, 评估总分为 500 分。通过评审的生产单位得分应不少于 350 分。
- b) 本表涉及的指标分项, 其相关信息可依据申请材料现场核查, 或要求生产单位现场提供或签署。
- c) 本表涉及的生产单位信息及评审情况不得对外泄露。

表 A.1 商用密码产品生产和保障能力评分表

受理单编号	生产单位名称		所属省(区、市)			受理时间	
申请型号产品	名称	功能	应用领域		研发、市场或其他方面优势特点		
评审时间		评估总分		是否存在关键项否决	<input type="checkbox"/> 是 <input type="checkbox"/> 否	评审组签字	
评分指标		评价标准及评分指南				信息来源	
1. 基本项(关键指标)*							
指标	指标分项	评价标准		评分指南		信息来源	达标情况
法人资格	—	是否在中国境内注册的独立法人。		在中国境内注册的独立法人。		申请材料	
主要技术人员	—	是否能满足人员要求。		从事密码产品设计、实现、检测或测试、技术支持等工作的主要技术人员应不少于 15 人, 并提供相关信息和社保缴纳证明。		申请材料	
产品研发	—	申请产品是否具有自主知识产权。		申请产品应具有自主知识产权, 且密码核心技术禁止外包或贴牌。		现场签署	
行业管理遵从项	—	是否同意承诺提供源代码或接受源代码现场审查, 是否同意承诺配合管理部门的市场监管和现场抽检。		承诺提供源代码或接受源代码现场审查, 配合管理部门的市场监管和现场抽检。		现场签署	

表 A.1 (续)

2. 声明项					
指标	指标分项	指标内容		信息来源	备注
关键人员	—	生产单位应提供关键人员的证件类型和号码、国籍、教育背景和从业经历的详细介绍。		申请材料	格式见 A.3
单位性质	—	生产单位应提供单位性质的声明,按照合法营业执照的内容如实提供,包括注册资本结构、注册资金规模、投资人名称、投资比例等。如有自然人,应说明自然人人数、姓名、国籍;如有外资成分,说明外资比例及外资参与公司经营管理的状况。		申请材料	格式见 A.4
数据管理	—	生产单位应提供数据中心所在地的声明,说明数据中心所在地、数据流转是否会涉及出境等情况。		申请材料	格式参见 A.5
3. 评估项-生产能力(200分)				该类总分:	
指标	指标分项	评价标准	评分指南	信息来源	分项评分
技术力量 (125分)	人力资源	是否设置研发、生产和管理关键岗位,并对担任该岗位的人员能力设置要求。 满分:15分	1) 生产单位设置了研发、生产和管理关键岗位,该项5分; 2) 关键岗位宜由经验丰富、专业技术深厚的资深人员担任,该项5分; 3) 生产单位的岗位设置齐备合理、任职资格清晰,该项5分。	申请材料+现场问卷、询问	
	主要技术团队	是否具备掌握与所申请许可专业或者产品相适应的关键技术的核心带头人,是否具备一定数量的密码技术研发、测试、技术支持人员团队。 满分:15分	1) 核心技术带头人信息安全行业从业经历5年以上,高级工程师或者硕士学位以上,研究成果获得省部级以上奖项的,每项5分;最高不超过10分; 2) 能够承担主要业务的专业技术人员15~30人,其中大学本科(含)以上学历所占比例不低于80%,该项2分; 3) 能够承担主要业务的专业技术人员≥30人,其中大学本科(含)以上学历所占比例不低于80%,该项3分。	申请材料	

表 A.1 (续)

指标	指标 分项	评价标准	评分指南	信息 来源	达标 情况
技术力量 (125 分)	技术积累 及优势	所申请的专业或产品是否与生产单位的科研方向符合、是否具备相关科研成果和技术储备,以及专业技术的水平高低。 满分:20 分	1) 申请许可的专业或者产品与生产单位的科研方向相符合或有偏差但可调整,该项 0~5 分; 2) 有与所申请许可专业相关领域的专业技术研究成果且该成果得到过应用,该项 0~5 分; 3) 近 3 年来开展过与所申请许可专业或者产品类似项目的科研且有技术储备,该项 0~5 分; 4) 专业技术水平满足所申请许可专业或者产品的需求且达到国内先进水平,该项 0~5 分。	现场 询问	
	技术创新	生产单位应具备授权专利、软件著作权、集成电路版图布图登记等; 生产单位应明确申请产品由省部级及以上单位或行业协会组织的专家鉴定结论为填补国内或国际行业应用空白; 生产单位应明确申请产品是否具备高性价比,是否具有良好的市场发展空间。 满分:40 分	1) 每个授权发明专利 2 分(2 个受理发明专利等同 1 个授权发明专利),每个授权实用新型专利 1 分(2 个受理实用新型专利等同 1 个授权实用新型专利),每个著作权或集成电路布图登记 1 分(每 2 个著作权申请或集成电路布图登记申请等同 1 个著作权或登记),该项最高 10 分。 2) 填补国内行业应用空白,该项 0~10 分,填补国际行业应用空白,该项 11~15 分。 3) 产品竞争力在性价比、性能、拓展市场空间等方面有创新,该项 0~15 分。	申请 材料 或现场 提供	
	研发工具 与设备	生产单位应具备满足申请产品研发需求的软硬件工具和设备。 满分:25 分	1) 具备申请许可的专业或者产品相关技术的关键研发工具,如研发工作站、研发专用软件、开发板、仿真器等,该项 0~15 分; 2) 具备申请许可的专业或者产品相关技术的关键研发设备,如示波器、逻辑分析仪等,该项 0~10 分。	申请 材料	
	试验测试 条件	生产单位应具有完善的密码产品功能、性能、稳定性、可靠性、环境适应性(如电磁兼容)等试验或测试条件。 满分:10 分	1) 具备密码产品功能、性能试验测试条件,该项 0~6 分; 2) 具备密码产品稳定性、可靠性、环境适应性试验测试条件,该项 0~4 分。	申请 材料 +现场 询问	

表 A.1 (续)

指标	指标分项	评价标准	评分指南	信息来源	达标情况
生产管理 (40分)	岗位设置	生产单位应设置生产主管、仓储管理员等相关岗位,并对担任该岗位的人员能力设定要求。 满分:10分	1) 设置了生产主管、仓储管理员等相关岗位,该项5分; 2) 规定了担任该岗位的人员能力设定要求,该项3分; 3) 规定了该岗位的职责、权限,且规定合理,该项2分。	申请材料	
	规章制度	生产单位应制定相应生产管理规章制度和仓库管理制度,并建立生产记录档案且确保生产记录可查询和追溯。 满分:10分	1) 制定了生产管理制度和仓库管理制度,制度完善,具有可执行性,该项5分; 2) 建立生产记录档案,确保生产记录可查询和可追溯,生产记录保持5年,该项5分。	申请材料	
	管理系统	生产单位应建立完善的产品出入库记录档案和数量管理系统,并确保数量管理系统的准确性。 满分:5分	建立完善的产品出入库记录档案和数量管理系统,且数量管理系统准确可靠,该项5分。	申请材料	
	供应管理	生产单位应考核供应商或外协单位是否具备相应的资质和技术能力,应要求供应商或外协单位提供资质和能力证明材料; 生产单位应对供应商供货环节和外协加工环节具备控制和监管措施,对供应商及外协加工产品提供质量标准并对供应商及外协产品生产的质量进行监视、测量和验收; 生产单位应与供应商签订质量保证协议并定期进行质量审查; 生产单位对外包人员、过程 and 外包工作有明确管理规定。 满分:15分	1) 是否考核了供应商或外协单位具有的资质或技术能力,并提供外协单位的资质和能力证明,该项4分; 2) 是否有部门负责外协单位质量的监视、测量和验收以及负责提供外加工产品的质量标准,对外协加工过程进行控制,该项4分; 3) 定期与供应商进行质量审查,签订质量保证协议,该项3分。 4) 对外包人员、过程及外包工作项有明确的管理规定,该项4分。	申请材料	
生产条件 (15分)	生产场所	生产单位的生产场所土地及房屋权属、生产设施、仓储场所应满足需求。 满分:10分	1) 生产单位拥有生产场所产权,该项5分;只具有租赁合同,该项3分; 2) 基础设施(如水、气、电供应设施等)满足需求,该项1分; 3) 支持性服务设施(如运输、通讯、信息化手段等)满足需求,该项1分; 4) 仓储场所满足需求:环境整洁,符合产品安全存储的环境条件要求,该项3分。	申请材料	

表 A.1 (续)

指标	指标分项	评价标准	评分指南	信息来源	达标情况
生产条件 (15分)	生产设备	生产单位应具备满足生产要求的生产设备和检测设备。 满分:5分	所需的生产辅助工具,加工、试验、检测设备,以及计量器具等通用设备满足需要,该项0~5分。		
生产工艺 与流程 (20分)	生产技术管理	生产单位应具备齐全的生产技术文件、管理规范。 满分:10分	1) 具有完备的生产技术文件,包括生产清单、生产指引或物料单或BOM清单,该项5分; 2) 具有出厂检验流程及报告文件,该项5分。	申请材料	
	批量生产和检测能力	生产单位应具备批量生产和检测能力,具备全自动化生产线及相应的产品检测机制,以保障产能充足、产品质量稳定;具备规定的检验、试验和计量设备,以满足与生产规模相适应的需要。 满分:10分	1) 具备全自动化生产线以及相应的产品检测机制,能够保障产能充足,产品质量稳定,该项5分; 2) 具备规定的检验、试验和计量设备,满足生产需要,与生产规模相适应,该项5分。	申请材料	
4. 评估项-质量保障能力(100分)				该类总分:	
指标	指标分项	评价标准	评分指南	信息来源	分项评分
管理规章制度 (25分)	—	生产单位应建立质量管理制度,明确质量目标并落实实施; 生产单位应保证商用密码产品的质量,设立质量管理岗位并明确岗位职责,在商用密码产品生产过程中应建立各阶段的质量目标并由生产单位高层负责实施; 生产单位应建立服务质量保障体系,明确对服务质量的标准要求,对服务质量进行监督并评估,为使用单位提供必要的技术保障服务。 满分:25分	1) 组织建立各阶段的质量目标并由高层负责牵头落实,该项4分; 2) 组织建立质量管理的标准及要求,该项4分; 3) 组织有专职的岗位负责质量控制并明确岗位职责,该项4分; 4) 组织对质量活动实施和控制方法,该项4分; 5) 组织有实施过程的质量职能,该项4分。 6) 组织建立完善的服务管理保证体系,该项2分; 7) 在服务体系中对服务质量标准有要求,该项2分; 8) 组织建立有服务质量监督制度,并对服务质量监督进行评估,该项1分。	申请材料	

表 A.1 (续)

指标	指标分项	评价标准	评分指南	信息来源	达标情况
开发过程管理 (45分)	开发与测试体系	是否建立了完备的开发体系。 满分:20分	1) 是否建立完备的开发体系:包括软件开发编码规范、系统集成设计管理规范、系统集成工程管理办法、软件开发管理规范、软件开发技术文档管理规范、软件变更管理规范,该项10分; 2) 是否建立了完备的测试体系:包括单元测试、集成测试、系统测试和验收测试,该项10分。	申请材料	
	研发过程管理	是否对研发过程进行管理和控制,以保证产品质量。 满分:15分	1) 是否遵循合理的研发流程,对产品研发过程有明确的阶段划分和过程管理规定,该项5分; 2) 研发过程中是否有架构设计、概要设计和详细设计方案,该项5分; 3) 定期对项目进行审核及评审,研发过程中是否有人去负责跟踪和组织协调,该项2分; 4) 具备变更管理规范,对变更产品及项目进行有效的管控,该项2分; 5) 建立技术文档管理规范,对技术性文档进行归档,该项1分。	申请材料	
	版本管理	对产品版本进行有效管理。 满分:10分	1) 制定有配置管理制度,该项5分; 2) 配备配置管理人员,该项3分; 3) 使用配置管理工具,该项2分。	现场提供	
质量问题管理 (10分)	—	是否对质量问题具有管理和控制措施,并就质量问题的解决进行跟踪管理。 满分:10分	1) 建立了质量问题处理工作流程和制度,该项3分; 2) 对问题处理时效性有要求,该项3分; 3) 定期执行客户满意度调查,该项2分; 4) 对问题处理有跟踪,对质量问题有统计的能力,该项2分。	申请材料	
持续改进产品质量措施 (10分)	—	是否有合理的持续改进产品质量的措施。 满分:10分	1) 持续性的产品质量跟踪监控,该项3分; 2) 收集产品质量改进的信息数据,该项3分; 3) 制定合理的产品质量改进计划,该项4分。	申请材料	

表 A.1 (续)

指标	指标分项	评价标准	评分指南	信息来源	达标情况
质量管理体系认证 (10分)	—	质量管理体系认证。 满分:10分	如企业通过 ISO 9001 质量体系认证、CMMI 3 软件开发成熟度认证等质量管理体系认证中至少一项,并且在有效期内,该项10分。	申请材料	
5. 安全保障能力(150分)				该类总分:	
指标	指标分项	评价标准	评分指南	信息来源	分项评分
组织保障 (40分)	领导力承诺	企业领导是否重视生产及管理安全。 满分:5分	主要领导承诺保证安全生产和明确信息安全的重要性,该项5分。	申请材料	
	建立组织机制	建立完善的组织机制,保证密码研发、生产安全。 满分:20分	1) 建立组织范围内的信息安全目标,该项4分; 2) 建立完善的组织机制,保证生产安全和信息安全,该项4分; 3) 成立专门的信息安全组织并明确信息安全的分工和责任,该项4分; 4) 定期进行组织内部信息安全管理制度的审核和评审,该项4分; 5) 建立组织预防、处理安全事件机制,该项4分。	申请材料	
	人力资源安全	具有保障人力资源安全的措施 满分:15分	1) 与员工签署正规的劳动合同并对员工进行信息安全培训,该项4分; 2) 相关岗位员工签署保密合同或合同中包含着信息安全条款并对相关岗位员工进行商用密码条例的培训,该项4分; 3) 对于离职的员工归还信息资产,撤销访问权限的规定,该项4分; 4) 对纠正(危害)信息安全的行为进行适当的鼓励(惩罚),该项3分。	现场提供	

表 A.1 (续)

指标	指标 分项	评价标准	评分指南	信息 来源	达标 情况
安全管理 (90分)	安全生产 规章制度	建立完善的安全生产管理 满分:20分	1) 建立安全生产规章制度并贯彻执行,该项2分; 2) 了解国家和行业的安全生产规定和标准,制定安全生产责任制和安全操作流程,该项2分; 3) 设置产品生产区域为重要区域,建立巡检制度,配备安全监督员或明确安全责任人,该项2分; 4) 生产单位应提供必要的岗前培训及安全生产培训,该项2分; 5) 为员工提供必要的安全和劳动保障措施和服务,该项2分。 6) 通过消防机构验收,该项2分; 7) 为生产场所配置完备的消防设施,对生产人员进行消防培训,该项2分; 8) 保证生产场所具有充足通畅的消防通道供生产人员安全撤离,该项2分; 9) 定期对机房防火、防雷、防漏、防尘等规程进行检查和记录,该项2分; 10) 在办公场所安装报警系统和灭火器,该项2分。	申请材料	
	物理和 环境安全	物理和环境的安全可靠 满分:8分	1) 划分安全区域,并规定相应责任人,定期对机房防盗、防尘、防磁、防静电按规程进行检查和记录,该项2分; 2) 重要区域有门禁系统及可查询的访问记录,有监控且记录保存30天以上,该项2分; 3) 重要资产进出具有审批机制,该项2分; 4) 重要区域,比如机房环境,具备温度和湿度要求、UPS不间断电源等,该项2分。	申请材料	

表 A.1 (续)

指标	指标 分项	评价标准	评分指南	信息 来源	达标 情况
安全管理 90 分	计算机和 网络安全	保障计算机和网络安全 满分:16 分	1) 具备恶意软件防护措施,该项 2 分; 2) 具有网络防护措施,如正确配置防火墙等,该项 2 分; 3) 重要信息资产具有专人维护,如源代码服务器、防火墙设备等,该项 2 分; 4) 制定有远程以及移动办公,建立安全管理制度或条款,该项 2 分; 5) 具备风险预警及应急处理措施,该项 2 分; 6) 建立有相适应的信息安全策略,该项 2 分 7) 保证信息存储、交换、销毁过程中的信息安全,该项 2 分; 8) 具有灾备计划和管理突发性信息安全事件的能力,该项 2 分。	申请材料	
	访问控制	安全有效的访问控制 满分:10 分	1) 具有独立的研发生产专用局域网,该项 4 分; 2) 如使用互联网,其接入要求受控,信息访问具有访问策略,该项 3 分; 3) 关键数据要进行安全的传输、接收和处理,及时删除存储介质上的数据或销毁存储介质,并详细记录存放信息,该项 3 分。	申请材料	
	介质控制	有效的介质管理 满分:8 分	1) 具有移动存储介质安全管理制度,该项 2 分; 2) 对存储介质有申请、使用、更换、维修及报废的安全管理制度和安全策略,该项 2 分; 3) 对关键存储介质有定期检查的记录,该项 2 分; 4) 对可重复利用的介质,执行写操作,覆盖旧内容,确保不可恢复;对于不再利用的介质采用毁损的方式进行物理销毁,确保不可恢复,该项 2 分。	申请材料	

表 A.1 (续)

指标	指标 分项	评价标准	评分指南	信息 来源	达标 情况
安全管理 (90分)	开发和支 持过程中 的安全	保障开发和支持过程中的安全 满分:12分	1) 具有开发安全制度或条款,该 项3分; 2) 具有项目开发安全风险识别 和控制措施,该项2分; 3) 具有配置管理或权限控制措 施,该项2分; 4) 外协/外包如果涉及商业秘密, 必须签署保密协议,该项3分; 5) 外协/外包环节不包含密钥安 装及关键参数配置,该项2分。	申请 材料	
	资产管理	保障资产安全 满分:4分	1) 具备识别所有资产并保持对 重要资产的保护,该项2分; 2) 制定一套与本单位所采用的 资产管理分类方案一致的信息 标识和处理程序并实施,该项 2分。	申请 材料	
	日志审计	保障日志安全 满分:6分	1) 对用户活动、意外和安全事件 日志、系统管理员和系统操作者 的活动进行记录,且按照约定的 期限对记录进行保存,该项 2分; 2) 保护日志设施和日志信息免 受破坏和未授权的访问,该项 2分; 3) 对错误日志进行分析并采取 适当的措施,该项2分。	申请 材料	
	事故管理	对安全事故有效预防及管理 满分:4分	1) 确保与信息系统有关的安全 弱点和安全事件的内部沟通并 及时采取相应措施,该项2分; 2) 使用持续有效的方法管理安 全事故,该项2分。	申请 材料	
	业务持续 性管理	保持业务持续可管理 满分:2分	防止业务活动中断并保护关键 业务流程不受信息系统重大失 效或自然灾害影响,确保及时恢 复,该项2分。	申请 材料	
信息安全 体系认证 (20分)	安全体系 认证	安全体系认证 满分:20分	通过信息安全体系 ISO 27001 认 证,并在有效期之内,该项 20分。	申请 材料	

表 A.1 (续)

6. 服务保障能力(50分)				该类总分:	
指标	指标分项	评价标准	评分指南	信息来源	分项评分
制度保障 (5分)	—	制定有服务保障规范 满分:5分	制定有技术保障、应急响应、产品售后等相关服务规范,该项5分。	现场提供	
应急响应能力 (20分)	—	具有应急响应机制,有解决突发问题的能力 满分:20分	1) 具有应急响应机制,对突发问题提供技术服务与解决方案,该项12分; 2) 在解决过程中及时向用户报告进展和最新状态,该项8分。	现场提供	
服务方式 (20分)	服务网络	具有相应的服务网络 满分:10分	1) 服务网络完善,结合产品应用情况提供符合需求的服务,该项5分; 2) 企业产品技术服务应明确承诺内容和可操作的服务方案,该项5分。	现场提供	
	受理与反馈	可提供多种服务受理与反馈方式 满分:10分	1) 建立官方的受理渠道,客户可通过呼叫中心、网络、当地客服部门等多种方式提出意见和问题,企业为用户来函反映、投诉的记录、处理和分析报告规定,该项5分; 2) 建立官方的反馈渠道和客户档案,并进行客户满意度调查,该项5分。	现场提供	
服务管理体系认证 (5分)	体系认证	具有相应的体系认证 满分:5分	通过 ISO 20000 认证,并在有效期之内,该项5分。	现场提供	

A.2 关键人员登记

关键人员登记表见表 A.2。

表 A.2 关键人员登记表

姓名		性别		职位	
国籍				人才类型	若为外籍人士是否是引进人才如： 千人计划、杰出青年学者等
证件类型	<input type="checkbox"/> 身份证 <input type="checkbox"/> 护照 <input type="checkbox"/> 港澳台证件 <input type="checkbox"/> 其他（请注明）			证件号码	
教育背景： 从高中学习开始至最高学历获得，包括全日制或在职教育					
从业经历： 请详细说明工作单位名称、起始时间、职位、工作方向、工作内容及成果。					
本人保证以上所述情况无误，均为本人真实经历。 本人无任何违法记录或受到过行政处罚。					
签字：					

A.3 单位性质说明

单位性质说明表见表 A.3。

表 A.3 单位性质说明表

单位名称		组织机构代码	
单位性质	<input type="checkbox"/> 央企 <input type="checkbox"/> 国企 <input type="checkbox"/> 民营企业 <input type="checkbox"/> 合资企业 <input type="checkbox"/> 外企 <input type="checkbox"/> 其他（请注明）	注册资金	<input type="checkbox"/> _____万元人民币 <input type="checkbox"/> _____万美元
资本结构			
投资人姓名	（如不止一人请自行增加）	投资比例	（如不止一人请自行增加）
自然人情况说明： （请如实说明自然人人数、姓名、国籍等信息）			
外资成分说明： （请如实说明外资比例及外资参与公司经营管理情况）			
本单位保证以上所述情况无误，均为真实情况。 法人代表签字：			

A.4 数据管理说明

数据管理说明表见表 A.4。

表 A.4 数据管理说明表

单位名称		组织机构代码	
数据管理说明： （请如实说明数据中心所在地、数据流装及数据流转是否出境等情况）			
本单位保证以上所述情况无误，均为真实情况。 法人代表签字：			

附 录 B
(规范性附录)

商用密码产品生产和保障能力评估报告

受理单编号：

生产单位名称		单位类型	(按照营业执照填写)	所属省(区、市)	
申请产品名称		产品类型		评估时间	20××年 月 日
评估材料是否齐全	<input type="checkbox"/> 是 <input type="checkbox"/> 否	基本项是否符合要求	<input type="checkbox"/> 是 <input type="checkbox"/> 否	现场审查	<input type="checkbox"/> 是 <input type="checkbox"/> 否
声明项说明	关键人员	是否持有外国国籍、绿卡、港澳台籍：_____			
	资本结构	是否有违法犯罪记录：_____			
	数据管理	投资比例			
评估项说明	生产能力	数据中心所在地：_____			(得分)
	质量保障能力	数据流转是否出境：_____			(得分)
	安全保障能力				
	服务保障能力				
	综合得分				
评估结论	<p>我单位组织评审组,按照标准要求对×××商用密码产品生产和保障能力进行评估,经评审,该单位_____ (具有/不具有)_____产品相适应的生产和保障能力。</p> <p>评估人员(签字):</p> <p style="text-align: right;">评估单位(加盖公章) ××××年××月××日</p>				
评估监督人员	<p>本次评审过程规范、公正,评估人员独立评分,未发现漏项,未发生违法、违规现象。本次评估结论真实有效。</p> <p style="text-align: right;">评估监督人员(签字):</p>				

附 录 C
(资料性附录)
审 核 方 法

本附录给了常用的审核方法说明。

选择审核方法取决于所规定的审核目标、范围和准则以及持续的时间和地点。应考虑审核人员能力和应用审核方法出现的任何不确定性,灵活运用各种不同的审核方法及其组合,可以使得审核过程及其结果的效率和有效性最佳化。

审核评估绩效与受审核管理体系的相关人员的相互作用和审核所用技术有关。可以单独或者组合地运用表 C.1 提供的审核方法示例以实现审核目标。如果一次审核使用多名成员组成的审核组,可以同时使用现场和远程的方法。

表 C.1 实用的审核方法

审核人员与被审核方之间的 相互组作用程度	审核人员的位置	
	现场	远程
有人员互动	进行面谈; 在被审核方参与的情况下完成检查表和问卷表; 在被审核方参与的情况下进行文件评审; 抽样	借助交互式的通信手段: ——进行交谈; ——完成检查表和问卷; ——在受审核方参与的情况下进行文件评审
无人员互动	进行文件评审(提交的申请资料、记录、数据分析); 观察工作情况; 进行现场巡视; 完成检查表; 抽样(产品)	进行文件评审(例如申请资料、记录、数据分析); 在考虑社会和法律法规要求的前提下,通过监视手段来观察工作情况; 分析数据
<p>现场审核活动在被审核方的现场进行。远程审核活动在受审核方现场以外地方进行,无论距离远近。</p> <p>互动的审核活动包括被审核人员和审核组之间的相互交流,非互动的审核活动不存在被审核方代表的交流,但需要使用设备、设施和文件。</p>		

附 录 D
(资料性附录)
归档材料清单

归档材料至少包括：

- a) 商用密码产品生产和保障能力评分表；
- b) 关键人员登记表；
- c) 单位性质说明表；
- d) 数据管理说明表；
- e) 商用密码产品生产和保障能力评估报告。

附录 E
(资料性附录)
重要领域产品使用要求

本附录给出了重要领域产品使用要求。

《中华人民共和国网络安全法》第三十一条规定,国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的关键信息基础设施,在网络安全等级保护制度的基础上,实行重点保护。

《中华人民共和国密码法》(草案)第十八条规定,国家对关键信息基础设施的密码应用安全性进行分类分级评估,按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查。

使用单位根据应用场景及安全保护要求选择不同安全等级商用密码产品。

结合声明项关键人员、单位性质、数据管理可能存在的不可控风险,推荐的系统安全等级保护要求与商用密码产品选用关系参见表 E.1。

应用于重要领域以及关键信息基础设施中的商用密码产品应参见表 E.1,选择不低于等级保护三级的产品。

使用单位应根据生产单位注册资本结构和注册资金规模,评估其是否具备商用密码产品服务、升级及新产品研制的的能力。

使用单位可参照 GM/T 0065—2019 对商用密码产品提供单位的生产与保障能力进行评估,评估合格后方可采购和使用。

使用单位参考商用密码产品提供单位的声明项信息选用产品,主要包括商用密码产品提供单位的关键人员信息、单位性质、数据管理情况。

表 E.1 系统安全等级保护要求与商用密码产品选用关系

声明项	属性	情况	系统安全等级保护要求				
			一级	二级	三级	四级	五级(待定)
关键人员	国籍	外国国籍	√				
		外国绿卡	√				
		大陆	√	√	√	√	√
		港澳台	√	√			
单位性质	股本结构	境内资本 100%	√	√	√	√	√
		境内资本 ≥51%	√	√	√		
		境内资本 <51%	√	√			
		境外资本 100%	√				
数据	数据中心	境内	√	√	√	√	√
		境外	√				
	数据流转	境内	√	√	√	√	√
		经境外	√	√			

参 考 文 献

- [1] GB/T 19000—2015 质量管理体系 基础和术语
 - [2] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
 - [3] GM/T 0039—2015 密码模块安全检测要求
 - [4] ISO/IEC 20000 信息技术服务管理规范 Information Technology Service Management
 - [5] ISO/IEC 27001 信息安全管理体系标准 Information Security Management System
 - [6] 商用密码管理条例[Z].1999-10.
 - [7] 商用密码产品生产管理规定[Z].2017-12.
 - [8] 《商用密码知识与政策干部读本》编委会.商用密码知识与政策干部读本[M].北京:人民出版社,2017.
 - [9] 中华人民共和国网络安全法
 - [10] 中华人民共和国密码法(草案)
-