ICS 35.040
L 80

GM

中华人民共和国密码行业标准

GM/T 0065—2019

商用密码产品生产和保障能力建设规范

Specification for capability construction 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

本标准根据 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：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、兴唐通信科技有限公司、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：周建锁、叶枫、赵闪、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，商用密码产品研制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。

为了对商用密码产品生产单位的生产和保障能力建设提供统一、客观的标准，为了生产单位对自身技术力量、场所、设备、生产工艺和质量保证能力有较为全面的把握，制定本标准。本标准从评估的角度对商用密码产品生产单位相关能力建设提出要求，也可用于第三方机构对商用密码产品生产单位进行评估。建设规范包含本标准和《商用密码产品生产和保障能力建设实施指南》，本标准规定了基本项、声明项和评估项等要素及要求；《商用密码产品生产和保障能力建设实施指南》包含评估方法、评估程序、评估报告和实施要点。

商用密码产品生产和保障能力建设规范

1 范围

本标准规定了商用密码产品生产和保障能力的评估要素和评估要求。

本标准适用于对商用密码产品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能力建设及核查。

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/Z 4001 密码术语

商用密码管理条例

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

主要技术人员 main technical personnel

从事商用密码产品设计、实现、检测或测试及技术支持工作的人员。

3.2

关键人员 crucial personnel

包括法定代表人、实际控制人、高层管理人员、技术负责人。

3.3

关键岗位 crucial position

对研发、生产和管理活动具有重要作用，对结果的质量有显著影响，甚至能决定结果成败的岗位。

3.4

密码核心技术 core cryptographic technology

商用密码产品中使用的实现密码核心功能的技术。

3.5

密码固件 cryptographic firmware

密码边界内的硬件中、执行期间不能被动态写入或修改的程序与数据组成部分。如存储硬件，包括但不限于 ROM、PROM、EEPROM 与 FLASH。

4 评估要素

4.1 基本项

基本项是商用密码产品生产单位应达到的基本条件，包括法人资格、主要技术人员、研发产品和行

业管理遵从项。

4.2 声明项

声明项是商用密码产品生产单位做出的特别说明，包括生产单位关键人员信息、单位性质和数据管理。

4.3 评估项

评估项是商用密码产品和生产保障能力评估的具体量化指标，生产单位参照评估项提高自身的商用密码产品生产和保障能力。

评估要求具体指标参见表1。

表1 评估指标

一级指标	二级指标	三级指标
生产能力	技术力量	人力资源
		主要技术团队
		技术积累及优势
		技术创新
		研发工具和设备
		试验测试条件
	生产管理	岗位设置
		制度保障
		管理系统
		供应管理
	生产条件	生产场所
		生产设备
		生产外协
	生产工艺与流程	生产技术管理
		批量生产和检测能力
		生产外协
质量保障能力	制度保障	
	开发过程质量管理	开发与测试体系
		研发过程管理
		版本管理
	质量问题管理	
	持续改进产品质量措施	
安全保障能力	组织保障	领导力承诺
		建立组织机制
		人力资源安全

表 1（续）

一级指标	二级指标	三级指标
安全保障能力	安全管理	安全生产制度保障
		物理和环境安全
		计算机和网络安全
		访问控制
		介质控制
		开发和支持过程中的安全
		资产管理
		日志审计
		事故管理
		业务持续性管理
服务保障能力	制度保障	
	应急响应能力	
	服务响应方式	服务网络
		受理与反馈

5 基本项要求

5.1 法人资格

应为在中国境内注册的独立法人。

5.2 主要技术人员

应不少于 15 人。

5.3 产品研发

产品密码核心技术应具有自主知识产权，禁止核心技术外包或产品贴牌。

5.4 行业管理遵从

应遵守商用密码产品管理相关法律法规，自愿遵从商用密码产品管理相关标准规定，并承诺提供产品源代码以供审查，承诺接受研发和生产现场审查，做好产品销售情况日常记录。

6 声明项要求

6.1 关键人员信息

应提供关键人员的国籍（或绿卡）、教育背景和从业经历等信息。若关键人员有违法犯罪记录，应如实声明。

6.2 单位性质

应声明单位性质信息，明确注册资本构成及注册资金规模。

6.3 数据管理

应声明商用密码产品研发、生产和保障数据中心所在地，并说明商用密码产品研发、生产和保障数据流转审批流程及数据流转是否经境外。

7 评估项要求

7.1 生产能力

7.1.1 技术力量

7.1.1.1 人力资源

应设置研发、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。

7.1.1.2 主要技术团队

a) 应具备能支撑密码产品研发的技术团队；
b) 应具备技术负责人，且技术负责人应掌握密码产品的关键密码技术。

7.1.1.3 技术积累及优势

a) 密码产品应符合生产单位的科研方向；
b) 在近5年内开展过与密码产品类似项目的科研活动并获得科研成果，有密码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；
c) 生产单位专业技术水平满足密码产品的需求或达到国内先进水平。

7.1.1.4 技术创新

a) 具有发明专利、实用新型专利、软件著作权和/或集成电路布图登记等知识产权；
b) 密码产品宜填补国内外行业应用空白，且产品在成本、功能、性能、可靠性、市场应用等方面具有竞争力和创新性。

7.1.1.5 研发工具和设备

应具备满足密码产品研发需求的软硬件工具和设备。

7.1.1.6 试验测试条件

应具有完善的密码产品功能、性能、稳定性、可靠性、环境适应性等试验或测试条件。

7.1.2 生产管理

7.1.2.1 岗位设置

应设置生产主管、仓储管理等相关岗位，并对担任该岗位的人员能力设定要求。

7.1.2.2 制度保障

应制定生产管理规章制度和仓储管理制度，并建立生产过程记录档案且确保生产过程记录可查询和追溯。

7.1.2.3 管理系统

a) 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) 应建立产品数量管理要求，并确保数量管理的准确性。

7.1.2.4 供应管理

a) 对供应商或外协单位应考核是否具备相应的资质和技术能力，要求供应商或外协单位提供资质和能力证明材料；
b) 对供应商供货环节和外协加工环节应具备控制和监管措施，对供应商及外协加工产品提出质量标准要求，并对供应商及外协产品生产的质量进行监视、测量和验收；
c) 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、过程和外包工作有明确管理规定。

7.1.3 生产条件

7.1.3.1 生产场所

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与产品生产能力相适应的需要。

7.1.3.2 生产设备

应具备满足生产要求的生产设备和检测设备。

7.1.3.3 生产外协

应提供生产外协单位满足 7.1.3.1 和 7.1.3.2 要求的证明材料。

7.1.4 生产工艺与流程

7.1.4.1 生产技术管理

应具备齐全的生产技术文件和管理规范。

7.1.4.2 批量生产和检测能力

应具备批量生产和检测能力，具备自动化生产线及相应的产品检测机制，具备规定的检验、试验和计量设备并与生产规模相适应。

7.1.4.3 生产外协

应提供生产外协单位满足 7.1.4.1 和 7.1.4.2 要求的证明材料。

7.2 质量保障能力

7.2.1 制度保障

应保证商用密码产品的全生命周期质量，建立质量管理制度及标准要求，明确质量目标并由高层管

理人员负责落实实施。

7.2.2 开发过程质量管理

7.2.2.1 开发与测试体系

应建立完备的开发与测试体系，规范芯片开发、软硬件模块开发和系统集成，规范单元测试、集成测试、系统测试和验收测试等活动。

7.2.2.2 研发过程管理

a) 对研发过程应进行管理和控制，对整个过程有明确的阶段划分和过程管理，具备变更管理规范并对变更进行管控；
b) 应建立技术文档管理规范并对技术性文档进行保存。

7.2.2.3 版本管理

对产品版本应进行管理并制定版本管理制度，设置版本管理人员，使用版本管理工具，保证每个产品版本与实际用户使用产品版本相对应，留存试用备品。

7.2.3 质量问题管理

a) 对质量问题应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) 应建立质量问题处理制度和流程，对质量问题处理的时效性进行要求。

7.2.4 持续改进产品质量措施

a) 应具有合理的持续改进产品质量的措施；
b) 对产品质量应进行持续跟踪监控并收集产品质量改进信息，且据此制定产品质量改进计划；
c) 应对客户进行产品质量满意度调查。

7.3 安全保障能力

7.3.1 组织保障

7.3.1.1 领导力承诺

应明确安全的重要性，建立组织范围内的安全目标，由高层管理人员承诺保证安全研发和生产。

7.3.1.2 建立组织机制

a) 应由专人或部门(组织)负责安全；
b) 应定期进行组织内部安全管理制度的审核和评审，确保安全管理体系的适宜性和有效性；
c) 应建立组织预防、处理安全事件的机制。

7.3.1.3 人力资源安全

a) 应与员工签署正规的劳动合同并对员工进行安全培训；
b) 应与相关岗位员工签署保密合同或合同中包含着安全管理条款，并对相关岗位员工进行商用密码相关法律法规的培训；

c) 对离职或调离岗位的单位员工应设置归还信息资产和撤销访问权限的规定；
d) 对纠正和危害安全的行为可进行适当的鼓励和惩罚。

7.3.2 安全管理

7.3.2.1 安全生产制度保障

a) 应建立安全生产规章制度并贯彻执行；
b) 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。

7.3.2.2 物理和环境安全

a) 应划分物理安全区域并任命相应的负责人；
b) 在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；
c) 在重要区域应安装监控系统且监控的内容记录可查询；
d) 对重要资产进出单位或重要区域应实行审批机制；
e) 对重要区域应设置温湿度要求并配备不间断电源；
f) 应通过消防机构认证，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，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；
g) 应由安全负责人定期对机房防火、防雷、防漏、防尘、接地等规程进行检查和记录。

7.3.2.3 计算机和网络安全

a) 应具备计算机软件防护措施和网络防护措施；
b) 重要信息资产应由专人维护；
c) 有远程及移动办公，应建立安全管理制度；
d) 应具备风险预警及应急处置措施；
e) 应建立适应组织的信息安全策略，保证信息存储、交换和销毁等过程中的安全；
f) 应具有重要数据备份机制及应急灾备计划。

7.3.2.4 访问控制

a) 应建立信息访问控制机制，对重要区域有识别并重点保护；
b) 对通过网络接入生产单位内网应有访问控制，具有员工对信息访问的控制策略；
c) 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；
d) 应详细记录数据存放信息。

7.3.2.5 介质控制

a) 应具有针对移动存储介质的安全管理制度；
b) 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安全策略，并保存对关键存储介质定期检查的记录；
c) 对可重复利用的介质应执行写操作以覆盖旧内容并确保不可恢复；
d) 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。

7.3.2.6 开发和支持过程中的安全

a) 应设立开发安全制度；

b) 应具有项目开发安全风险识别和控制措施，具有配置管理或权限控制措施；
c) 外协/外包过程如涉及商业秘密应签署保密协议，且外协/外包过程应不包含密钥安装及关键参数配置。

7.3.2.7 资产管理

a) 应识别所有的资产并保持对重要资产的保护；
b) 应制定一套与生产单位所采用的资产管理分类方案一致的信息标识和处置程序并实施。

7.3.2.8 日志审计

a) 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应进行记录，且按照约定的期限对记录进行保存；
b) 应保护日志设施和日志信息免受破坏和未授权的访问；
c) 对错误日志应进行分析并采取适当的措施。

7.3.2.9 事故管理

a) 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；
b) 对安全事故应使用持续有效的方法管理。

7.3.2.10 业务持续性管理

应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。

7.4 服务保障能力

7.4.1 制度保障

a) 应设置完善的服务保障制度，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。
b) 根据服务管理的策划应实施服务管理并提供服务、监督、测量和评审，并持续改进。

7.4.2 应急响应能力

a) 应建立应急响应机制并统筹规划、协调管理；
b) 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并最小化对业务的影响；
c) 在解决过程中应及时向用户报告进展和最新状态。

7.4.3 服务响应方式

7.4.3.1 服务网络

a) 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) 应明确产品技术服务承诺内容和可操作的服务方案。

7.4.3.2 受理与反馈

a) 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；

b） 对用户来函反映及投诉问题应记录，明确问题处理期限，并将相应处理的结果形成报告；

c） 应建立客户档案；

d） 对客户应进行服务质量满意度调查。