



T/MITEC 015-2023

商用密码产业人才岗位要求

Industrial Talents Competency Framework of Commercial Cipher

2023-10-09 发布

2023-10-09 实施

工业和信息化部人才交流中心 发布

目 次

前 言 1

1 范围 2

2 术语和定义 2

3 商用密码主要方向及岗位 2

 3.1 主要方向 3

 3.2 主要岗位及职责 3

4 商用密码产业人才岗位能力要素 4

5 商用密码产业人才岗位要求 4

 5.1 研发设计方向岗位能力要求 5

 5.2 集成应用方向岗位能力要求 7

 5.3 密码测评方向岗位能力要求 8

 5.4 服务推广方向岗位能力要求 9

附 录 A （资料性附录） 商用密码产业人才岗位能力提升 12

附 录 B （资料性附录） 商用密码产业人才岗位能力评价 14

参 考 文 献 15

前 言

本标准按照 GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本标准由工业和信息化部人才交流中心提出并归口。

本标准起草单位：工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心、工信通（北京）信息技术有限公司、北京国泰网信科技有限公司、渔翁信息技术股份有限公司、江苏意源科技有限公司、四川邮电职业技术学院。

本标准主要起草人：李学林、色云峰、程宇、李利利、李廷茹、付京波、陈子雄、李想、王斌、闫华旗、杨滨滨、李欣、李元正、遇君扬、郭刚、岳鹤涛、蒋日友、史瑀、唐伟、任勉、王太成。

本标准为首次制定。



商用密码产业人才岗位能力要求

1 范围

本标准规定了商用密码领域主要方向岗位能力要求。

本标准适用于指导相关单位开展商用密码人才培养、人才评价（人才认证）、人才招聘、人才引进等工作。

2 术语和定义

下列术语和定义适用于本文件。

2.1

商用密码 commercial cipher

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。

[来源：《商用密码管理条例》2023年4月27日中华人民共和国国务院令第760号修订]

2.2

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

[来源：GM/Z 0001-2013, 2.54]

2.3

算法标识 algorithm identifier

用于对密码算法进行唯一标识的符号。

[来源：GM/Z 0001-2013, 2.124]

2.4

密码测评 password assessment

指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性、有效性等进行评估。

[来源：霍伟、马原、郭启全.商用密码应用与安全性评估[M].北京：电子工业出版社，2020年]

3 商用密码主要方向及岗位

3.1 主要方向

党的十八大以来，我国商用密码管理和应用在法制化、规范化基础上，逐步向科学化、体系化方向迈进。深化商用密码管理改革，强化商用密码自主创新，推进商用密码合规、正确、有效应用是新时期商用密码发展面临的重要任务。2023 年 7 月 1 日，新版《商用密码管理条例》正式实施，并强调重点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。根据商用密码全产业链应用需求，本标将准聚焦商用密码研发设计、集成应用、密码测评、服务推广四个方向岗位。

商用密码研发设计是确保密码产品安全性、可靠性和合规性的关键环节，涵盖密码应用总体规划设计、密码算法与协议实现、密码设备设计、密码操作系统开发、密码系统集成和测试等内容。商用密码集成应用是将密码技术应用到实际系统中，对保护敏感信息安全、抵御各种网络攻击等具有重要作用，具体涵盖密码方案设计和仿真应用等内容。

商用密码测评是对商用密码产品提供的安全功能进行核验的有效手段，对规范密码应用以及维护网络与信息系统密码安全，切实保障网络安全，具有至关重要的实际作用，具体包括安全等级符合性检测和功能标准符合性检测两方面内容。

商用密码服务推广是为用户提供全面支持和有效服务，确保密码产品稳定性和安全性，提高用户满意度和信任度，促进密码技术的广泛应用，具体包括装配调试、运维服务和人员培训等内容。

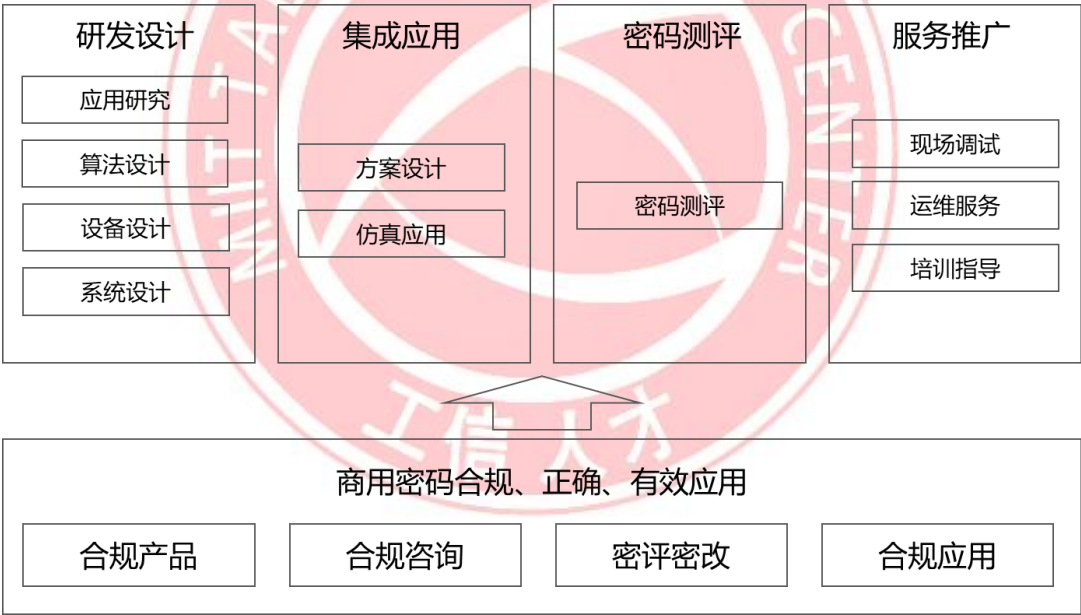


图 1 商用密码主要方向岗位框架图

3.2 主要岗位及职责

本标准主要涉及以下商用密码产业岗位，具体如表1所示。

表 1 商用密码产业各方向主要岗位及职责

序号	方向	岗位名称	岗位职责
1	研发设计	规划设计工程师	负责研究商用密码理论和前沿技术，规划、设计、审定商用密码方案，并制定持续改进策略。

2		密码算法工程师	负责分析、设计、实现符合标准和规范要求的密码算法和协议。
3		密码设备设计工程师	负责设计、开发商用密码设备技术方案，实现功能模块和接口的开发，并编制审定安全设计文档和测试方案。
4		密码系统开发工程师	负责设计、开发、评估商用密码系统，编制审定详细设计，并持续优化系统以满足业务需求。
5		测试工程师	负责制订产品质量与性能的测试与检定方案，进行产品检测、质量评估，完成产品认证。
6	集成应用	解决方案工程师	负责根据客户需求和现场条件，设计合理的系统的整体方案，包括集成、调试、优化等。
7		仿真工程师	负责应用仿真软件和工具平台，进行结构设计、运动控制、轨迹规划与高层次逻辑算法有效性保障等工作。
8	密码测评	商用密码测评工程师	负责对不同领域信息系统开展密码应用性测评工作。
9	服务推广	装调工程师	负责应用现场设备安装及系统调试。
10		售后服务工程师	负责产品调整、故障诊断、维护，并提供客户售后支持及反馈改进建议。
11		培训师	负责商用密码培训、教学及相关的指导工作。

4 商用密码产业人才岗位能力要素

本标准按照专业知识、技术技能、工程实践、综合能力四个维度提出了商用密码产业人才岗位能力要素。

表2 商用密码产业人才岗位能力要素列表

维度	要素	说明
专业知识	基础知识	指相应岗位人才应掌握的通用知识，主要包括基本理论、相关标准与规范知识以及有关法律法规、安全、隐私等。
	专业知识	指相应岗位人才完成工作任务所必备的知识，主要指与具体岗位要求相适应的理论知识、技术要求和操作规程等。
技术技能	基本技能	指相应岗位人才为完成工作任务所应具备的对基础知识应用的水平以及熟练程度。
	专业技能	指相应岗位人才为完成工作任务所应具备的对专业知识应用的水平以及对特殊工具使用的掌握。
工程实践	经验	指相应岗位人才在实际工程与项目推进中应当具备的经验。
综合能力	软能力	指相应岗位人才为完成工作任务所应具备的行为特征和综合素质，包括学习创新、沟通协调、团队协作、业务场景把握等能力，以及责任心、主动性、职业道德等素养。

5 商用密码产业人才岗位要求

5.1 研发设计方向岗位能力要求

5.1.1 总体规划设计工程师

a) 专业知识

- 熟悉常用的密码算法，包括SM1、SM7、SM2、SM3、SM4、SM9、ZUC算法等，并对算法的标准与规范有深度的理解；
- 熟悉计算机组成原理、计算机网络技术、操作系统应用、信息安全标准与法规；
- 熟悉密码技术中常用的多种密码协议，包括身份认证协议、密钥协商协议、电子支付协议等；
- 熟悉国内外密码标准、法律法规、政策规定，并有着一定的见解；

b) 技术技能

- 具备优秀的编程能力，熟悉Java、Python、C++或并发编程，具备代码优化能力；
- 熟悉密码和信息安全相关知识，熟悉PKI密码体系；
- 熟悉PKCS标准，熟悉GM接口；

c) 工程实践

- 具备商用密码应用成果展示与相关配套系统、工具的研发经验；
- 具备网络安全等级保护测评、风险评估、运维和安全集成实施经验；

d) 综合能力

- 熟悉商用密码行业国内外现状、应用场景和发展趋势；
- 了解国家数字化安全战略及建设规划，对商用密码产品所应用的密码技术有深入了解；
- 具备较强的学习能力，能在应用研究中运用所学习的新技术；
- 具备较强的管理能力、沟通能力及团队合作能力，并能在多学科背景团队中发挥作用。

5.1.2 商用密码算法工程师

a) 专业知识

- 熟练掌握常见的密码算法知识，包括对称密码算法、非对称密码算法、摘要算法；
- 熟练掌握密码算法参数与密钥知识，以及对应的相关标准；
- 熟练掌握FPGA原理及应用；
- 具备较好的数学理论基础与信息安全理论基础；
- 具备扎实的密码技术基础，熟悉国内和国际商用密码算法体系；
- 熟悉商用密码相关国家、行业及团体标准；

b) 技术技能

- 熟练掌握FPGA相关开发工具，熟悉常用的设计模式；
- 熟练掌握常见的密码学算法，包括DES、AES、RSA、ECC等；
- 熟练掌握各种安全假设，包括整数分解假设、RSA假设、离散对数假设；
- 熟练使用编程工具、继续集成、持续交付工具；
- 熟悉开源软件工作模式、掌握开源软件工具；

c) 工程实践

- 具备密码算法开发项目经验；
- 具备密码算法实施或集成产品的实施开发经验；
- 能够结合业务问题进行分析，设计、优化并实现密码算法和数据安全协议；

d) 综合能力

- 掌握常见的密码算法的功能需求，熟练运用密码编码和密码解析；
- 熟悉安全芯片侧信道攻击方法，熟悉SPA/CPA/DPA等攻击、分析、防护；
- 熟悉常用的国际与国密算法，具备密码算法的硬件实现能力及软件实现能力。

5.1.3 密码设备设计工程师

a) 专业知识

- 熟练掌握常见的密码算法知识，包括对称密码算法、非对称密码算法、摘要算法；
- 掌握密码算法参数与密钥知识，以及对应的相关标准；
- 熟练掌握FPGA原理及应用；
- 具备深入的网络和信息安全知识，了解常见的安全漏洞和攻击方式；

b) 技术技能

- 熟练掌握FPGA相关开发工具，熟悉常用的设计模式；
- 熟练掌握常见的密码学算法，包括DES、AES、RSA、ECC、Signature等；
- 熟练掌握各种安全假设，包括整数分解假设、RSA假设、离散对数假设；
- 熟练掌握至少一种编程语言，如C、C++、Java等；

c) 工程实践

- 能够对产品发展方向进行整体把控，根据市场进行分析，为现有产品增加所需功能；
- 能够根据需求撰写需求规格说明文档；
- 具备密码产品硬件、软件实现功能的经验；

d) 综合能力

- 能够结合需求，设计产品的使用场景、应用范围及主要功能；
- 熟练掌握密码卡产品的设计流程及方法。

5.1.4 密码系统开发工程师

a) 专业知识

- 熟练掌握信息系统安全知识，并根据安全等级进行密码系统集成建设方案的编制；
- 熟练掌握密码系统集成测试方法及测试工具；
- 能够识别系统运行过程中产生的问题及风险，并提供解决方法；
- 能够根据密码应用解决方案进行密码产品的选型；

b) 技术技能

- 熟练掌握密码产品选型知识；
- 熟练掌握系统测试方法；
- 熟练掌握系统试运行报告的编制规范；
- 能够根据密码应用解决方案核验密码产品安全、调试及应用的正确性；

c) 工程实践

- 具备丰富的密码集成测试方法，并能够实现具体测试方案；
- 能够结合实际业务问题进行分析、设计、优化测试方案；
- 具有物理和环境、网络和通讯、设备和计算、应用和数据等方面的集成经验；

d) 综合能力

- 具备相应的项目管理知识；
- 具备良好的沟通表达及团队合作能力；
- 熟悉密码产品整体设计流程及相应步骤；

——掌握集成测试编制规范、信息系统密码应用基本要求。

5.1.5 测试工程师

a) 专业知识

——熟悉加密算法、非对称加密算法、数字签名、杂凑算法等；
——熟悉常见的密码产品测试平台、工具，清楚平台测试目标；
——熟悉测试密码系统接口、功能和性能测试方法；
——掌握测试计划、测试用例及测试报告编制方法；

b) 技术技能

——熟练操作常用的操作系统，熟悉使用常用命令进行问题分析定位；
——具备Shell、Python等基础脚本编写能力；
——熟悉使用性能测试工具和自动化测试工具；
——能够进行测试需求分析，将输出自动化功能方案；
——熟悉制定和维护自动化测试方案；

c) 工程实践

——具备丰富的分布式系统项目经验，有分布式一致性或共识算法测试经验；
——能够对平台常见问题进行分析、定位，能够对性能瓶颈问题快速排除和定位；

d) 综合能力

——具备较强的学习能力，能快速掌握密码产品已有的测试方法，同时能探索业界更先进的测试流程；
——具备较强的表达能力，团队合作精神和沟通能力；
——具备快速学习新产品能力，能够对全新产品、平台开展测试；
——具备良好的文字表达能力，能够编制用户可操作的实践文档。

5.2 集成应用方向岗位能力要求

5.2.1 解决方案工程师

a) 专业知识

——熟悉相关的国内外监管法规、政策、密码体系安全动态及标准；
——掌握数据安全、密码安全等信息安全基础知识；
——熟悉常见应用系统软件架构及业务逻辑；
——熟悉常见数据库系统及大数据系统工作机制；
——熟悉密码学底层原理与实现，如常见算法原理及应用方式、PKI体系、数据加解密机制、签名/验签机制、身份认证机制、密钥管理体系等；
——熟悉密码学相关前沿技术领域，如安全多方计算协议、属性基加密、格密码、同态加密、差分隐私、零知识证明等；

b) 技术技能

——熟练掌握密码产品安全策略的制定执行逻辑；
——具备相关密码产品的工程经验与较强的密钥管理体系设计能力；
——熟练掌握身份认证、数据传输加密等密码协议的协议结构与应用方法；
——熟练掌握应用系统对各类密码资源的常见调用方式；
——熟悉信息系统密码资源融合部署的实施方法；
——熟悉信息系统密码资源运维管理方法；

c) 工程实践

- 具备梳理密码应用与业务系统联动接口的能力；
- 具备根据信息系统安全等级设计安全策略的能力；
- 具备根据业务场景设计密钥管理体系的能力；

d) 综合能力

- 具备分析系统业务场景密码应用需求能力；
- 具备依据业务需求，合理化选择密码技术及产品的能力；
- 具备良好的文档编写及沟通表达能力；
- 对常见密码产品形态有较深入的理解，能够结合具体业务实际开展工作。

5.2.2 仿真工程师

a) 专业知识

- 熟悉业务与产品相关的国内外监管法规、政策、密码体系安全动态及标准；
- 对常见密码产品形态有较深入的理解，能够结合具体业务实际开展工作；
- 掌握数据安全、密码安全等信息安全基础知识；
- 熟悉常见应用系统软件架构及业务逻辑；
- 熟悉常见数据库系统及大数据系统工作机制；
- 熟悉密码学底层原理与实现，如常见算法原理及应用方式、PKI体系、数据加解密机制、签名/验签机制、身份认证机制、密钥管理体系等；
- 熟练掌握身份认证、数据传输加密等密码协议的结构与应用方法；

b) 技术技能

- 熟练掌握密码产品安全策略的制定执行逻辑；
- 具备相关密码产品的工程实践经验与较强的密钥管理体系设计能力；
- 熟悉基本渗透测试方法，熟练掌握对各类密码安全机制的技术验证方法；
- 熟悉密码学相关前沿技术领域，如安全多方计算协议、属性基加密、格密码、同态加密、差分隐私、零知识证明等；

c) 工程实践

- 具备密码系统安装、调试、问题解决能力；
- 具备应急处置密码应用安全突发事件能力；
- 具备调试密码应用与业务系统联动接口的能力；
- 具备根据信息系统安全等级设计安全策略的能力；
- 具备对密码应用安全机制有效性和防护强度的技术验证能力；

d) 综合能力

- 具备分析系统业务场景密码应用需求能力；
- 具备依据业务需求，合理化选择密码技术及产品的能力；
- 具备对信息系统密码资源进行融合部署实施的能力；
- 具备对信息系统密码资源及应用进行运维管理的能力；
- 熟悉密码相关产品、系统的典型应用场景，具备软硬件的产品安装、网络联调、功能测试及其他技术支持能力；
- 对常见密码产品形态有较深入的理解，能够结合具体业务实际开展工作。

5.3 密码测评方向岗位能力要求

5.3.1 商用密码测评工程师

a) 专业知识

- 熟练掌握信息系统安全知识，并根据安全等级进行密码系统集成建设方案的编制；
- 熟练掌握密码系统集成测试方法及测试工具；
- 能够识别系统运行过程中产生的问题及风险，并提供解决方法；
- 熟练掌握《信息系统密码应用基本要求》；

b) 技术技能

- 熟练掌握密码产品选型知识；
- 熟练掌握总体测评、密码技术应用测评、密钥管理测评、安全管理测评的测评方法；
- 熟练掌握测评工具、抓取信息系统相关数据通过访谈、文档审查等方法进行现场测评工作；

c) 工程实践

- 具备丰富的商用密码应用性评估经验；
- 能够结合实际业务问题进行分析，设计优化测评方案；

d) 综合能力

- 具备分析系统业务场景密码应用需求能力；
- 具备依据业务需求，合理化选择密码技术及产品的能力；
- 具备对信息系统密码资源进行融合部署的部署的能力；
- 具备对信息系统密码资源及应用进行运维管理的能力；
- 熟悉密码相关产品、系统的典型应用场景，具备软硬件的产品安装、网络联调、功能测试及其他技术支持能力。

5.4 服务推广方向岗位能力要求

5.4.1 装调工程师

a) 专业知识

- 熟练掌握主流密码系统、产品的使用及安装流程；
- 熟练掌握密码产品内部系统语言、网络系统工具及测试工具；

b) 技术技能

- 具备编写技术实施方案、改造方案、运行调试记录的能力；
- 掌握业务系统和密码系统的接口调试、硬件调试、功能调试；
- 掌握Linux系统，熟悉Java语言，熟悉系统集成相关产品功能及技术应用；

c) 工程实践

- 具备密码系统安装、调试及问题解决能力；
- 具备业务系统涉及密码产品的上线、变更、应急、保障、巡检以及测试环境中非应急故障或问题的支持能力；
- 具备根据不同客户需求制定并实施综合性技术方案的能力；

d) 综合能力

- 具备良好的沟通能力、问题分析及处理能力；
- 熟悉密码相关产品、系统的典型应用场景，能够基于客户现场情况，完成软硬件的产品安装、网络联调、功能测试及其他技术支持。

5.4.2 售后服务工程师

a) 专业知识

- 熟悉常见的密码故障指令及维护方式；
- 熟悉密码应用方案编制与评审的要点；

- 熟悉对称加密、非对称加密算法、数字证书和数字签名的原理；
- 熟悉密码产品的运行机制，能够及时发现运行异常的表现形式；

b) 技术技能

- 具备扎实的编程能力，熟练使用Java、Python等编程语言；
- 熟练使用脚本、编程语言、日志分析等工具快速定位问题；
- 能够根据系统需要，制定监控方案、及时捕捉系统异常；
- 能够对密码系统运行策略进行优化改进，制定操作预案，撰写应急执行报告、组织应急处置演练；
- 能够组织损失评估工作，审核损失评估报告；
- 能够对应急预案外突发事件提出处置方案；

c) 工程实践

- 精通Linux系统运维，对Linux操作系统原理有一定的理解；
- 能够准确识别系统上不同数据隐患和安全需求；
- 熟练掌握信息系统安全等级，设计密码应用运维管理制度；
- 能够对密码系统执行状况进行精准评估；

d) 综合能力

- 具有产品常见故障诊断、解决能力；
- 具备良好沟通能力，能够对客户问题进行有效解答；
- 熟练掌握主流密码系统、产品的使用及安装流程；
- 具备良好的撰写能力，整理并编写客户售后日志。

5.4.3 培训师

a) 专业知识

- 熟悉商用密码产业发展趋势、行业知识与应用案例、商用密码主流技术体系；
- 熟悉密码学、应用数学、计算机基础等密码相关技术原理；
- 掌握商用密码课程开发方法；
- 掌握商用密码教学设计原理；
- 熟悉教育学、心理学、社会学等方面相关知识；
- 熟悉操作技能培训要点与要求；
- 熟悉培训质量管理知识；

b) 技术技能

- 掌握需求调研工具，如问卷法、访谈法等；
- 掌握常用的培训方案设计与课程开发工具，如ADDIE、PPT等；
- 熟悉常用的授课技巧，如TTT、SPOT引导技术；

c) 工程实践

- 具备商用密码相关培训需求的方案设计与实施经验；
- 具备教学实践经验，能够独立进行授课；
- 具备良好的文档撰写能力，能够完成培训需求说明书、咨询报告和教学方案等文档的编写工作；
- 具备一定的商用密码相关咨询经验；
- 能够组织开展技术改造、技术革新活动；

d) 综合能力

- 具备良好的学习能力，善于快速学习商用密码知识与技术，并进行转化、归纳总结；

- 具备良好的逻辑思维能力，能够输出结构化人才培养方案及课程体系；
- 具备良好的沟通能力，善于与需求方、学员进行沟通交流；
- 熟悉商用密码人才成长规律。



附 录 A
(资料性附录)
商用密码产业人才岗位能力提升

A.1 商用密码岗位能力提升内容

岗位能力提升内容应包括：

- a) 基础知识、专业知识等相关知识提升；
- b) 基本技能、专业技能等相关技术技能提升；
- c) 基于项目经验的工程实践能力提升；
- d) 软技能等相关综合能力提升。

A.2 商用密码岗位能力提升阶段和方式

商用密码岗位能力提升分为岗前提升和在岗提升两个阶段，构成商用密码相关岗位从业人员不同阶段和能力水平的终身教育体系。

- a) 岗前提升方式，包括：
 - 1) 理论教学；
 - 2) 理论与实践一体化教学；
 - 3) 项目实训、企业实习等方式。
- b) 在岗提升方式，包括：
 - 1) 内部在岗培训；
 - 2) 外部脱岗培训；
 - 3) 项目实践或导师辅导等。

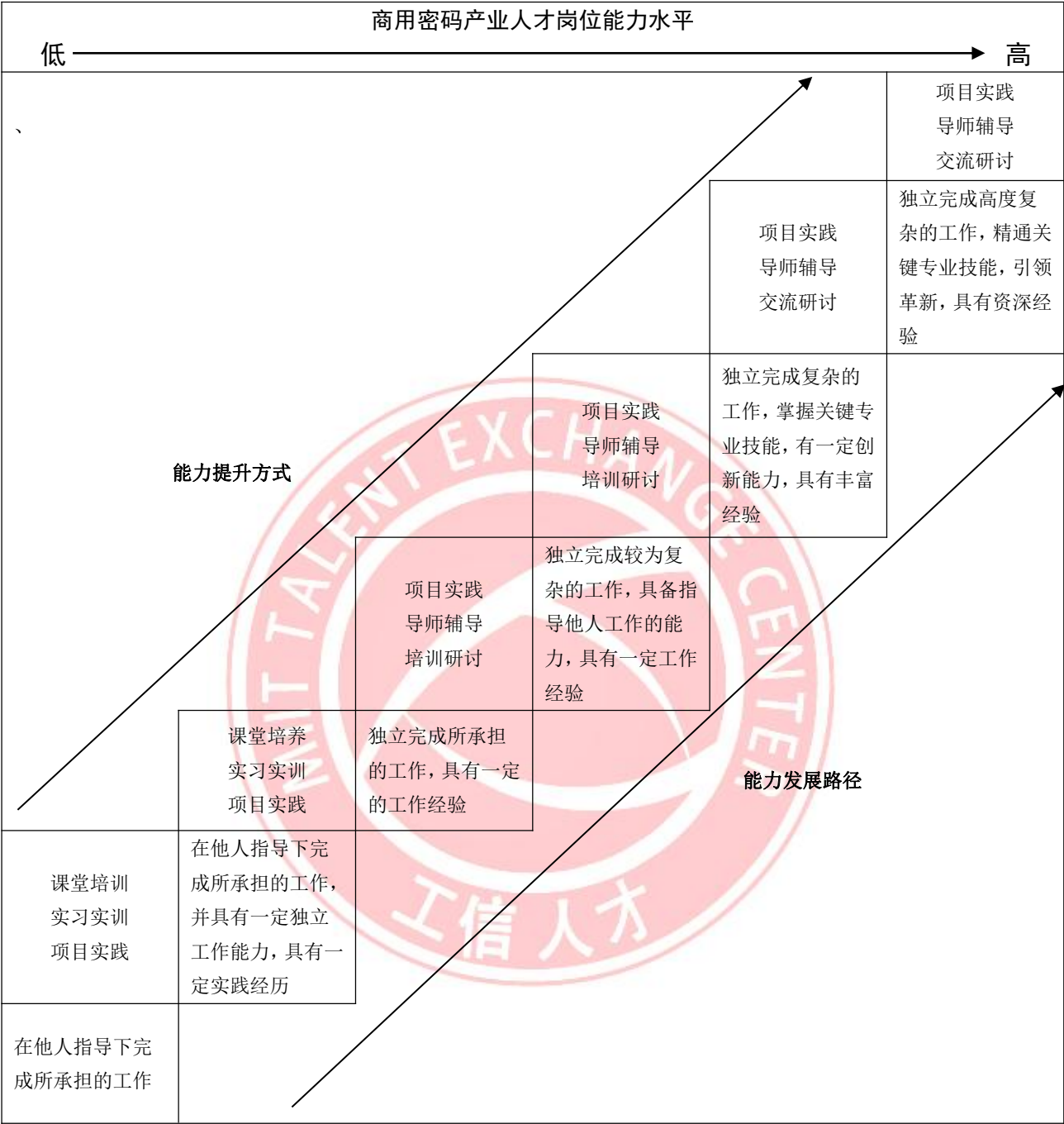
A.3 商用密码岗位能力提升活动供给类别

商用密码岗位能力提升活动供给包括：

- a) 教育、培训机构培养：符合要求的各级教育机构（普通高校、中等和高等职业院校等）及培训机构应根据商用密码各岗位能力要求，制定人才能力提升方案，为商用密码产业及企业培养合格的从业人员，满足个人发展需要；
- b) 企业培养：企业结合业务发展需要，应根据商用密码各岗位能力要求有针对性、有计划地实施岗位能力提升计划，满足个人发展需要，增强企业竞争力；
- c) 个人培养：从业人员根据个人发展计划，做好职业规划与岗位定位，对标商用密码岗位能力要求，不断积累提高综合能力，积累专业知识、技术技能和工程实践经验。

商用密码产业人才岗位能力提升路径见图A.1。

图A.1 商用密码产业人才岗位能力提升路径



附 录 B
(资料性附录)
商用密码产业人才岗位能力评价

B.1 商用密码产业人才岗位能力评价方法

对从业人员进行评价和定级，评价结果可以作为商用密码产业人才能力胜任、职业发展等活动的依据。评价方式包括：

- a) 专业知识主要通过笔试考核方式进行评价；
- b) 技术技能主要通过实验考核方式进行评价；
- c) 工程实践主要通过成果评价方式进行评价；
- d) 综合能力主要通过笔试或答辩等方式进行评价。

B.2 商用密码产业人才岗位能力评价等级

商用密码产业人才岗位能力评价等级可以分为初、中、高级三级，能力分为9等。

- a) 初级（1—3级）：在他人指导下完成所承担的工作，并具备一定独立工作能力，具有一定实践经历；
- b) 中级（4—6级）：独立完成较为复杂的工作，具备指导他人工作的能力，具有一定工作经验；
- c) 高级（7—9级）：独立完成高度复杂的工作，精通关键专业技能，引领革新，具有资深经验。

B.3 商用密码产业人才岗位能力等级评价权重

商用密码产业人才岗位能力等级评价权重表如下：

表B.1 商用密码产业人才岗位能力等级评价权重表

评价维度		专业知识	技术技能	工程实践/综合能力
岗位等级		评价分值权重		
高级	9 级	20%	30%	50%
	8 级			
	7 级			
中级	6 级	50%	25%	25%
	5 级			
	4 级			
初级	3 级	70%	25%	5%
	2 级			
	1 级			
备注		评价总分满分为 100 分，由专业知识、技术技能、工程实践、综合能力四项评价维度的权重总分所得。		

参 考 文 献

- [1] GM/Z 0001-2013 密码术语
- [2] 商用密码管理条例（2023年4月14日国务院第4次常务会议通过，2023年4月27日中华人民共和国国务院令第七60号）
- [3] 霍伟、马原、郭启全.商用密码应用与安全性评估[M].北京：电子工业出版社，2020年.
- [4] 商用密码知识与政策干部读本[M].北京：人民出版社，2017年.
- [5] 工业互联网产业联盟.工业互联网体系架构(版本1.0)[R/OL].(2017-02-08)[2020-04-22].
<http://www.aii-alliance.org/index.php?m=content&c=index&a=show&catid=23&id=24>

