ICS 35.240
CCS L80

T/CCUA

中 国 计 算 机 用 户 协 会 团 体 标 准

T/CCUA XXX-2023

流程工业企业 工业互联网数据安全保障 密码应用要求

Process industry enterprise—Industry internet data security insurance —Requirements of cryptography application

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

本稿完成日期：2023 年 10 月 12 日

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国计算机用户协会　发 布

目　　次

前　言

本文件按照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。

本文件与 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》共同构成流程工业企业工业互联网数据安全保障密码应用的协调配套标准。其中GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》是基础性标准，本文件是在GB/T 39786-2021基础上的进一步细化和扩展，根据流程工业企业工业互联网数据安全保障特点，提出和规定了流程工业企业工业互联网数据安全保障密码应用技术要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国计算机用户协会工业互联网与大数据分会标准化委员会工作组提出。

本文件由中国计算机用户协会归口。

本文件起草单位：中国计算机用户协会、华能信息技术有限公司、郑州信大云谷科技有限公司、中国电力科学研究院有限公司、×××。

本文件主要起草人：刘鲁清、李栋梁、周伟、唐慧林、高飞、尚宇炜、张钊、刘玥君、×××、×××

流程工业企业 工业互联网数据安全保障 密码应用要求

1 范围

本文件规定了流程工业企业工业互联网数据密码应用的基本原则、总体框架、通用要求、技术要求和管理要求。

本文件适用于指导流程工业企业工业互联网数据安全保障密码应用的规划、建设、运行及测评。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

流程工业 process industry

利用化学反应、分离或混合等技术手段制造新产品，改进已有产品或处理废弃物的工业。

注1：流程工业包含以下行业：化工，石油化工，废弃物处理，造纸及水泥行业等。

注2：流程工业不包括以下行业：装备，机械制造及其类似行业。也不包括有特殊要求或需要特殊批准的行业。

3.2

工业互联网 industrial internet

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系。

3.3

生产控制大区 production control zone

由具有数据采集与控制功能、纵向联结使用专用网络或专用通道的电力监控系统构成的安全区域。

3.4

管理信息大区 management information zone

生产控制大区之外的，主要由企业管理、办公自动化系统及信息网络构成的安全区域。

3.5

机密性 confidentiality

保证信息不被泄露给非授权实体的性质。

3.6

完整性 integrity

数据没有遭受以非授权方式所作的改变的性质。

3.7

真实性 authenticity

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

3.8

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

3.9

加密 encipherment; encryption

对数据进行密码变换以产生密文的过程。

3.10

密钥 key

控制密码算法运算的关键信息或参数。

3.11

密码基础设施 cryptography infrastructure

提供鉴别、加密、完整性和不可否认性服务的信息安全基础设施。

3.12

数字证书 digital certificate

具有权威性、可信性和公正性的证书认证机构（CA）进行数字签名的一个可信的数字化文件。

3.13

非可控网络 non-control network

运营主体不能确认其安全性的网络，包括但不限于专用有线通信网、公用通信网（如租用的运营商的专线、5G、卫星微波）等。

3.14

控制区 control sub zone

由具有实时监控功能、纵向联接使用电力调度数据网的实时子网或者专用通道的各业务系统构成的安全区域。

3.15

非控制区 non-control sub zone

在生产控制范围内由在线运行但不直接参与控制、是电力生产过程的必要环节、纵向联接使用电力调度数据网的非实时子网的各业务系统构成的安全区域。

3.16

非对称密码算法 asymmetric cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.17

身份认证 authentication

专用于确定传输、消息或发信方的有效性的安全措施，或者对接受特定的信息类别的个人授权进行验证的手段。

4 缩略语

下列缩略语适用于本文件。

CA：数字证书认证中心（Certificate Authority）

PKI：公钥基础设施（Public Key Infrastructure)

5 应用原则

5.1 流程工业企业工业互联网特性

流程工业企业工业互联网系统具有以下特性。

a) **可靠性**：流程工业企业工业互联网系统的可靠稳定运行是确保工业生产安全的基础，同时系统生产过程自身是连续不间断工作方式，对系统可用性要求高，不能暂停工作。

b) **实时性**：流程工业企业工业互联网系统中各个设备按照业务逻辑在固定时间完成特定动作，不能有丝毫差错，否则将威胁设备、系统的正常运行，甚至对物理世界产生破坏；流程工业企业工业互联网系统从过程数据的实时采集、传输到控制指令的下达执行，周期短。

c) **分布性**：流程工业企业工业互联网系统应具有实时闭环控制的特性，采集、传输、控制等业务模块采用地理或空间位置上的分散布置方式。

d) **系统性**：流程工业企业工业互联网系统在时间上应具有时变性和连续性，在空间上具有分布参数和分布处理的特性，在技术上涉及技术领域和设备系统较多，在管理上涉及业务部门和层级较多，对系统性要求很高。

e) **安全性**：流程工业企业工业互联网系统大量采用计算机及通信技术，应在保障生产过程功能安全的同时，确保系统及网络安全，将安全防护措施融入生产控制业务中，减少中间环节，提高重要工业控制系统的可靠性，安全措施应适应重要工业控制系统的实时性，网络安全防护应具有分布性和系统性。

5.2 流程工业企业工业互联网数据安全密码应用原则

结合流程工业企业工业互联网系统特性和面临网络安全威胁，流程工业企业工业互联网数据安全保障密码应用遵循以下基本原则。

a) **应用合规**：数据防护采用的密码算法、技术、产品和服务应遵守 GB/T 39786-2021 第 5 章规定的要求。

b) **策略可控**：采用密码机制对非可控网络中数据进行安全防护时，应由企业制定、管理密码防护策略，密钥和证书由企业密码基础设施管理。

c) **分类分级数据的密码保护**：在企业已实施数据分类分级标准的情况下，非密的各类安全等级的数据应采用合规的密码策略进行保护；涉密的，按相关管理制度和规范进行保护。

6 应用框架

6.1 密码应用总体框架

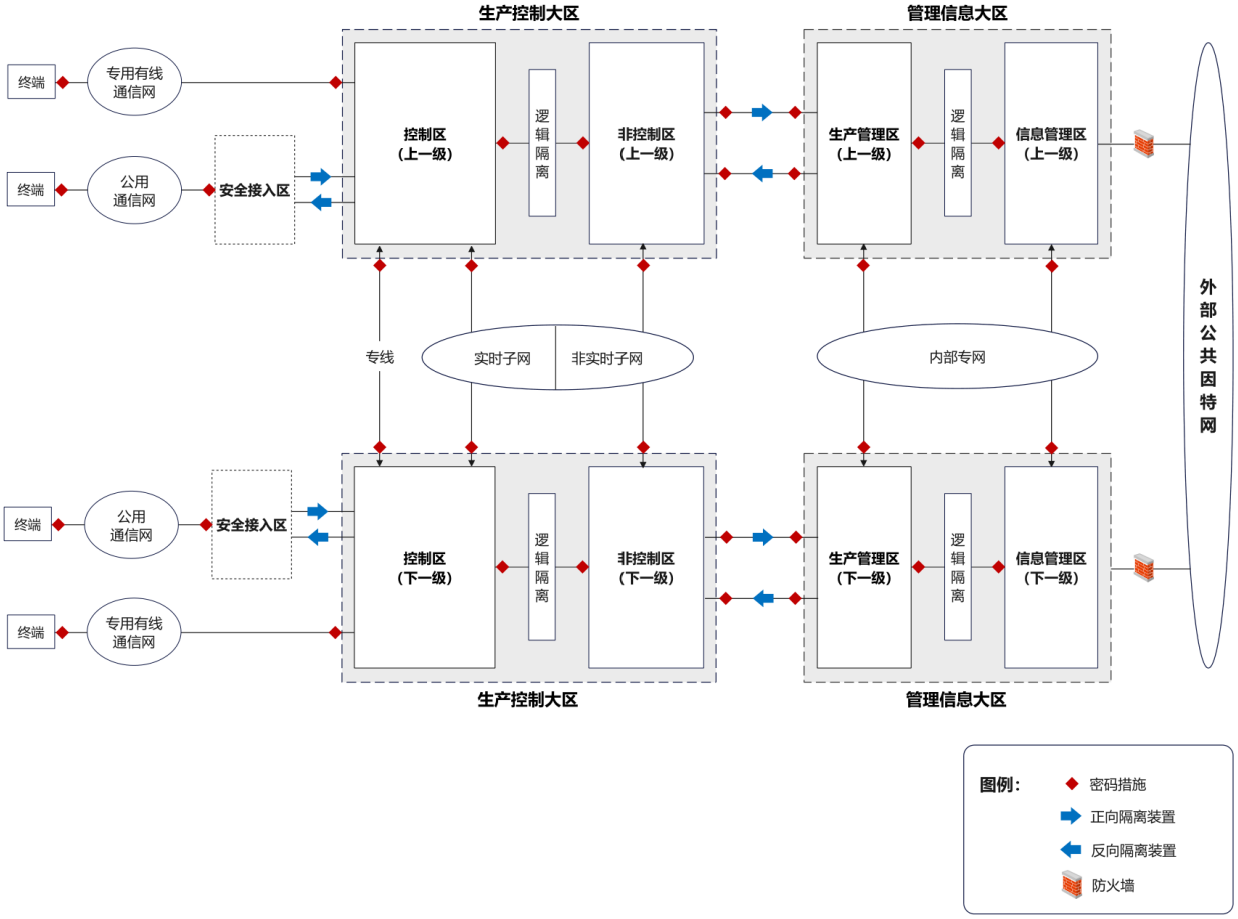

图1 流程工业企业工业互联网数据安全密码应用框架

流程工业企业工业互联网系统内部基于计算机和网络技术的业务系统，应划分为生产控制大区和管理信息大区（见图 1）。生产控制大区可以分为控制区(安全区 I)和非控制区(安全区 II)；管理信息大区内部在不影响生产控制大区安全的前提下，可以根据各企业不同安全要求划分生产管理区（安全区III）、信息管理区（安全区Ⅳ）等安全区。

生产控制大区中，宜将业务系统完整置于一个安全区内，但当业务系统的某些功能模块与此业务系统不属于同一个安全区内时，可将其功能模块分置于不同的安全区中；安全区之间数据通信，应通过密码措施实现数据的完整性、机密性保护。

控制区上下级之间数据通信使用实时子网或专用通道进行传输，应通过密码措施实现身份认证、数据的完整性和机密性保护；非控制区上下级之间数据通信使用非实时子网进行传输，应通过密码措施实现身份认证、数据的完整性和机密性保护；实时子网与非实时子网之间实现逻辑隔离。

生产控制大区与管理信息大区之间如需通信，应设置经国家指定部门检测认证的专用单向隔离装置，生产控制大区到管理信息大区的数据传输应采用正向隔离装置，并通过密码措施实现数据的完整性、机密性保护；管理信息大区到生产控制大区若有必要进行数据传输，应采用反向隔离装置，并通过密码措施实现数据的完整性、机密性保护。

生产控制大区的业务系统在与其终端的纵向联接中使用专用有线通信网或公用通信网进行通信的，两端均应采用相应的密码措施，实现双向身份认证、访问控制，以及数据完整性和机密性保护。其中，使用公用通信网进行通信的，应设立安全接入区，并通过单向隔离装置接入生产控制大区。

管理信息大区在通过内部专网与外部公共因特网进行数据传输时，应采用具备加密认证功能的防火墙，实现安全传输。

6.2 密码应用通用要求

流程工业企业工业互联网数据密码应用应满足以下通用要求：

a) 应构建密码服务基础设施，实现对称加解密、非对称加解密、哈希函数计算等密码运算功能，支持身份鉴别、加解密、完整性保护等服务。
b) 密码服务基础设施应支持国产非对称密码算法（SM2）标准、国产哈希函数算法（SM3）标准、国产对称密码算法（SM4）标准。
c) 密码服务基础设施应基于 PKI/CA 系统，为流程工业企业的用户、机构、设备、应用提供统一的数字证书发放和生命周期管理。
d) 密码服务基础设施应能够为流程工业企业的用户、机构、设备、应用提供身份认证功能，确保人员、机构、设备、应用身份的真实性、可信性。
e) 密码服务基础设施应具备密钥管理功能，提供统一的密钥生成和生命周期管理服务。

7 应用技术要求

7.1 流程工业企业工业互联网一般数据

7.1.1 数据采集

本级要求包括：

a) 可采用密码技术验证数据提供实体的身份；
b) 可采用密码技术保证数据的完整性；
c) 宜采用密码技术保证数据采集操作审计记录的完整性。

7.1.2 数据传输

本级要求包括：

a) 可采用密码技术保证传输过程中数据的机密性；
b) 可采用密码技术保证传输过程中数据的完整性；
c) 宜采用密码技术保证数据传输操作审计记录的完整性。

7.1.3 数据存储

本级要求包括：

a) 可采用密码技术保证存储过程中数据的机密性；
b) 宜采用密码技术保证数据存储操作审计记录的完整性。

7.1.4 数据处理

本级要求包括：

a) 可采用密码技术鉴别数据访问实体身份；
b) 宜采用密码技术保证数据处理过程审计记录的完整性。

7.1.5 数据交换

本级要求包括：

a) 可采用密码技术鉴别参与数据交换的实体身份，保证身份的真实性；
b) 可采用密码技术保证交换数据的完整性；
c) 宜采用密码技术保证数据交换过程审计记录的完整性。

7.1.6 策略管理

本级要求包括：
a) 可对密码策略进行基于平台的统一管理；
b) 宜采用密码技术保证密码策略操作审计记录的完整性。

7.2 流程工业企业工业互联网重要数据

7.2.1 数据采集

本级要求包括：
a) 应采用密码技术验证数据提供实体的身份；
b) 应采用密码技术保证采集数据的完整性；
c) 应采用密码技术保证数据采集操作审计记录的完整性；
d) 宜采用密码技术对采集数据进行安全标识；
e) 宜采用密码技术保证数据安全标记的完整性；
f) 宜采用密码技术提供数据原发证据和接收证据，实现数据原发行为和接收行为的不可否认性。

7.2.2 数据传输

本级要求包括：
a) 应采用密码技术保证传输过程中数据的机密性；
b) 应采用密码技术保证传输过程中数据的完整性；
c) 应采用密码技术保证数据传输操作审计记录的完整性；
d) 宜采用密码技术实现不同业务数据传输的信道隔离；
e) 宜采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。

7.2.3 数据存储

本级要求包括：
a) 应采用密码技术保证存储过程中数据的机密性；
b) 应采用密码技术保证数据存储操作审计记录的完整性；
c) 宜采用密码技术保证存储过程中数据的完整性。

7.2.4 数据处理

本级要求包括：
a) 应采用密码技术鉴别数据访问实体身份；
b) 应采用密码技术保证数据处理过程审计记录的完整性；
c) 宜采用密码技术保证数据在处理过程中的机密性；
d) 宜采用密码技术对数据访问和操作权限进行控制，限定用户可访问数据范围。

7.2.5 数据交换

本级要求包括：
a) 应采用密码技术鉴别参与数据交换的实体身份，保证身份的真实性；

b） 应采用密码技术保证交换数据的完整性；
c） 应采用密码技术保证数据交换过程审计记录的完整性；
d） 宜采用密码技术保证交换数据操作的可控性；
e） 宜采用密码技术防止数据交换造成用户隐私泄露；
f） 宜采用密码技术提供数据交换过程中的原发证据和接收证据，实现数据交换行为的不可否认性。

7.2.6 策略管理

本级要求包括：
a） 应对密码策略进行基于平台的统一管理；
b） 应采用密码技术保证密码策略操作审计记录的完整性；
c） 宜采用密码技术鉴别策略管理人员身份。

7.3 流程工业企业工业互联网核心数据

7.3.1 数据采集

本级要求包括：
a） 应采用密码技术验证数据提供实体的身份；
b） 应采用密码技术保证采集数据的完整性；
c） 应采用密码技术保证数据采集操作审计记录的完整性；
d） 应采用密码技术对采集数据进行安全标识；
e） 应采用密码技术保证数据安全标记的完整性；
f） 应采用密码技术提供数据原发证据和接收证据，实现数据原发行为和接收行为的不可否认性。

7.3.2 数据传输

本级要求包括：
a） 应采用密码技术保证传输过程中数据的机密性；
b） 应采用密码技术保证传输过程中数据的完整性；
c） 应采用密码技术保证数据传输操作审计记录的完整性；
d） 应采用密码技术实现不同业务数据传输的信道隔离；
e） 应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。

7.3.3 数据存储

本级要求包括：
a） 应采用密码技术保证存储过程中数据的机密性；
b） 应采用密码技术保证数据存储操作审计记录的完整性；
c） 应采用密码技术保证存储过程中数据的完整性。

7.3.4 数据处理

本级要求包括：
a） 应采用密码技术鉴别数据访问实体身份；
b） 应采用密码技术保证数据处理过程审计记录的完整性；
c） 应采用密码技术保证数据在处理过程中的机密性；
d） 应采用密码技术对数据访问和操作权限进行控制，限定用户可访问数据范围。

7.3.5 数据交换

本级要求包括：

a) 应采用密码技术鉴别参与数据交换的实体身份，保证身份的真实性；
b) 应采用密码技术保证交换数据的完整性；
c) 应采用密码技术保证数据交换过程审计记录的完整性；
d) 应采用密码技术保证交换数据操作的可控性；
e) 应采用密码技术防止数据交换造成用户隐私泄露；
f) 应采用密码技术提供数据交换过程中的原发证据和接收证据，实现数据交换行为的不可否认性。

7.3.6 策略管理

本级要求包括：

a) 应对密码策略进行基于平台的统一管理；
b) 应采用密码技术保证密码策略操作审计记录的完整性；
c) 应采用密码技术鉴别策略管理人员身份。

8 应用管理要求

8.1 管理制度

使用密码技术的流程工业企业应符合以下管理制度要求：

a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置等制度；
b) 应对管理人员、审计人员或操作人员执行的日常管理操作建立操作规程，应建立内部登记、权限管理与审批机制，明确密码应用安全授权审批事项、审批部门和审批人等，根据实际建立多级审核工作机制和流程；
c) 应明确密码应用管理责任部门，负责统筹开展密码应用管理工作，包括制定密码应用管理制度规范、组织开展密码应用安全评估、提出密码应用保护的对策建议、监督检查密码应用管理制度规范执行落实情况等；
d) 应制定存储介质安全管理方案，应采用安全存储技术妥善控制和保管各类介质，应对密钥介质的登记、出入库、领用和初始化等方面制定管理制度；
e) 应制定供应链安全管理方案，并明确供应链涉及的密码应用的安全风险控制措施；
f) 应建立数据安全审计相关制度，明确审计目的、审计对象、审计操作规程、审计频度、审计内容、审计报告要素等；
g) 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
h) 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
i) 应具有密码应用操作规程的相关执行记录并妥善保存。

8.2 人员管理

使用密码技术的流程工业企业应符合以下人员管理要求：

a) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
b) 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限如下：
   1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；

2) 对关键岗位建立多人共管机制；
3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；
4) 相关设备与系统的管理和使用账号不得多人共用；
5) 密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任，并应在任前对其进行背景调查。

c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
d) 应定期开展密码应用安全宣传教育与技能培训，提高人员密码应用安全意识和专业技能，定期对密码应用安全岗位人员进行考核；
e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

8.3 建设运行

建设运行要求包括：

a) 应依据密码相关标准和密码应用需求，制定密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行密码保障系统；
b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期；
c) 在数据分类分级定义的基础上明确提出对相关类型、级别的数据的加密传输要求，针对数据的加密传输要求应包含对数据加密算法要求和密钥的管理要求；
d) 建设密钥管理系统提供数据的加密解密、签名验签等功能，并实现对密钥的全生命周期的安全管理；
e) 应具备对数据收集行为进行监测的技术能力，并能够在发现异常时进行告警；
f) 应依据法律规定或者与用户约定的方式和期限存储数据，应采用校验技术、密码技术等措施进行安全存储；
g) 应根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应采取校验技术、密码技术、安全传输通道或者安全传输协议等措施保障数据传输；
h) 在运行过程中，应采用数据加密、容灾备份、访问控制、数据审计等手段，对数据的处理与应用进行基于密码的安全防护；
i) 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
j) 在运行过程中，对系统各阶段涉及的数据要采用基于国密算法的安全防护；
k) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估，并根据评估结果进行整改；
l) 应对联网工业控制网络安全区域之间及工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。

8.4 应急处置

应急处置要求包括：

a) 应制定密码应用应急预案，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时处置；
b) 应急处理预案应根据事件的严重程度、紧急程度和事件类别，分别规范告警、报告、保护、处置、善后、总结等处理流程和处置措施；
c) 事件发生后，应及时向信息系统主管部门及归属的密码管理部门进行报告；

d) 事件处置完成后，应在规定期限内形成总结报告，每年向有关部门报告密码应用安全事件处置情况。总结报告内容包括事件原因、事件后果、影响范围、事件责任、处置过程和结果、工作经验等；

e) 应针对应急事件处理中暴露的问题，不断完善和修改应急处理预案；

f) 应根据实际情况建设工业互联网密码应用风险监测预警能力，重点面向联网工业控制系统、工业交换机、工业数据服务器、工业网络边界、工业软件、工业数据库、工业云平台等开展密码应用风险监测，根据流程工业企业工业互联网密码应用特征及面临的典型风险进行针对性监测分析，排查安全隐患，采取必要措施防范密码应用风险。

8.5 应用测评

应用测评要求包括：

a) 在系统规划及建设阶段，应自行或者委托密码检测机构对密码应用方案进行密码应用安全性评估；

b) 信息系统建成运行后，应自行或者委托密码检测机构每年至少开展一次密码应用安全性评估，确保密码保障系统正确有效运行；

c) 开展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。

参 考 文 献

[1] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[2] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求
[3] GB/T 42021-2022 工业互联网 总体网络架构
[4] GM/T 0115—2021 信息系统密码应用测评要求
[5] GB/T 17901.1-2020 信息技术 安全技术 密钥管理 第1部分：框架
[6] GM/Z 4001—2013 密码术语
[7] GB/T 22135—2019 流程工业中电气、仪表和控制系统的试车 各特定的阶段和里程碑