ICS 35.030
CCS L80

团　体　标　准

T/TAF 347—2026

面向端云协同机密计算的远程证明技术要求

Technical requirements for remote attestation of end-cloud collaborative confidential computing

2026-06-17 发布　　2026-06-17 实施

电信终端产业协会　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。

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。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：小米通讯技术有限公司、中国信息通信研究院、荣耀终端股份有限公司、北京抖音信息服务有限公司、OPPO广东移动通信有限公司、国民认证科技（重庆）有限公司、安谋科技（中国）有限公司、维沃移动通信有限公司、玩咖欢聚科技（北京）有限公司、中兴通讯股份有限公司、北京快手科技有限公司、每日互动股份有限公司。

本文件主要起草人：顾泽宇、袁琦、王艳红、赵晓娜、吴博峰、杜蕾、李根、付艳艳、李俊、王俊超、武林娜、杜云、陈鑫爱、姜峰、黄丹、赵光晞、田琛、郑琛、李美慧、吴宗锦、刘俊伟、赵盈洁、张宏伟、落红卫、王昕、李颖莹。

引　言

移动智能终端厂商和物联网厂商的端云协同计算场景下，基于硬件信任根的机密计算来保护运行时数据的安全，在性能和安全性中取得了很好的平衡，应用越来越广泛。端云协同场景在机密计算应用过程中，需要针对端云协同场景的特点，拓展传统机密计算定义中的方案设计，以实现向终端用户证明当前云端计算环境的机密性，数据处理过程可追溯可审计，以满足隐私合规要求。本文件从机密计算应用的架构和实现上给出适用于端云协同场景的技术要求。

面向端云协同机密计算的远程证明技术要求

1 范围

本文件规定了端云协同场景下，使用机密计算远程证明开放平台的安全性并实现端云可信通信的架构、流程和基本要求，包括设备端功能、云端功能、安全性等方面的技术要求。

本文件适用移动智能终端厂商和物联网厂商及监管机构，在实施或者评估机密计算数据保护能力的时候，对于远程证明设计实施方案的审核。

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 25069—2022 信息安全技术 术语

GB/T 45230—2025 数据安全技术 机密计算通用框架

3 术语和定义

下列术语和定义适用于本文件。

3.1

机密计算 confidential computing

在可信的硬件基础上，通过隔离、加密、证明、封装等机制，保护使用中数据安全的计算模式。。

[来源：GB/T 45230—2025，3.3]

3.2

远程证明 remote attestation

对机密计算环境和机密计算应用程序进行完整性校验和身份认证的过程，向验证者提供可信的状态报告。

4 缩略语

下列缩略语适用于本文件。

CBOR：简洁二进制对象表示（Concise Binary Object Representation）

HSM：硬件安全模块（Hardware Security Module）

JWT：JSON网络令牌（JavaScript Object Notation Web Token）

RATS：远程证明令牌服务（Remote Attestation Token Service）

RBAC：基于角色的访问控制模型（Role-Based Access Control）

TCB：可信计算基（Trusted Computing Base）

TLS：传输层安全协议（Transport Layer Security）

5 面向端云协同机密计算的远程证明参考架构和流程

本文给出面向端云协同机密计算的远程证明参考架构如图 1 所示，包括设备端和云端两个部分。主要实现以下能力。

a） 验证云端服务可信性：远程证明服务能够为端侧设备提供云端服务可信状态的验证，确保只有可信服务才能给端侧提供服务，防止用户数据泄露。

b） 确保端云通信安全：通过安全通信通道，保障端侧设备与云端之间的数据传输不被窃取或篡改，为机密数据的传输提供可靠的通信环境。

c） 保护数据机密性：设备端和云端对数据进行加解密处理，确保数据在传输和存储过程中的机密性，只有授权的设备端和云端才能解密和访问数据。

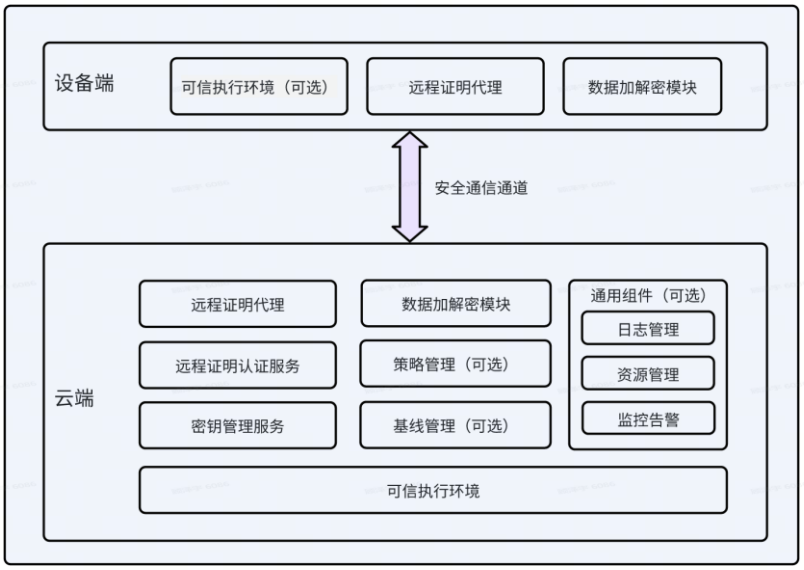


图 1 面向端云协同机密计算的远程证明参考架构

面向端云协同机密计算的远程证明具体执行流程如图 2 所示。

云端执行流程如下。

a） 云端业务应用程序从密钥管理服务获取集群内公用的密钥，该密钥支持定期轮换。

b） 云端远程证明代理获取当前集群部署节点的远程证明报告，根据实际业务需要，宜将集群公钥追加到远程证明报告中。

c） 云端远程证明认证服务对上述报告完成认证，密钥管理服务通过加密机私钥对认证结果进行签名，生成 JSON Web Token（JWT），保存在云端远程证明代理中。

设备端执行流程如下。

a） 设备端远程证明代理向云端远程证明代理发起认证请求，获取 JWT、集群公钥、证书链，使用加密机公钥验证 JWT 的合法性，校验通过后将集群公钥保存在设备端加解密模块，该集群公钥用于派生后续端云传输业务数据使用的加密密钥。具体密钥派生过程可参考附录 A。

注：设备端远程证明代理根据实际业务场景，可以触发云端远程证明代理按照云端执行流程中所述步骤生成新的机密计算认证结果，也可以直接复用云端远程证明代理周期性生成并缓存的机密计算认证结果。

b） 设备端业务 APP 调用设备端加解密模块，使用加密密钥对业务数据进行加密，发送给云端业务应用程序。

c) 云端业务应用程序，调用云端加解密模块，解密请求数据，使用明文在机密计算节点中执行计算，将计算结果调用云端加解密模块进行加密后返回给业务 APP。

d) 设备端业务 APP，调用设备端加解密模块，解密返回结果。

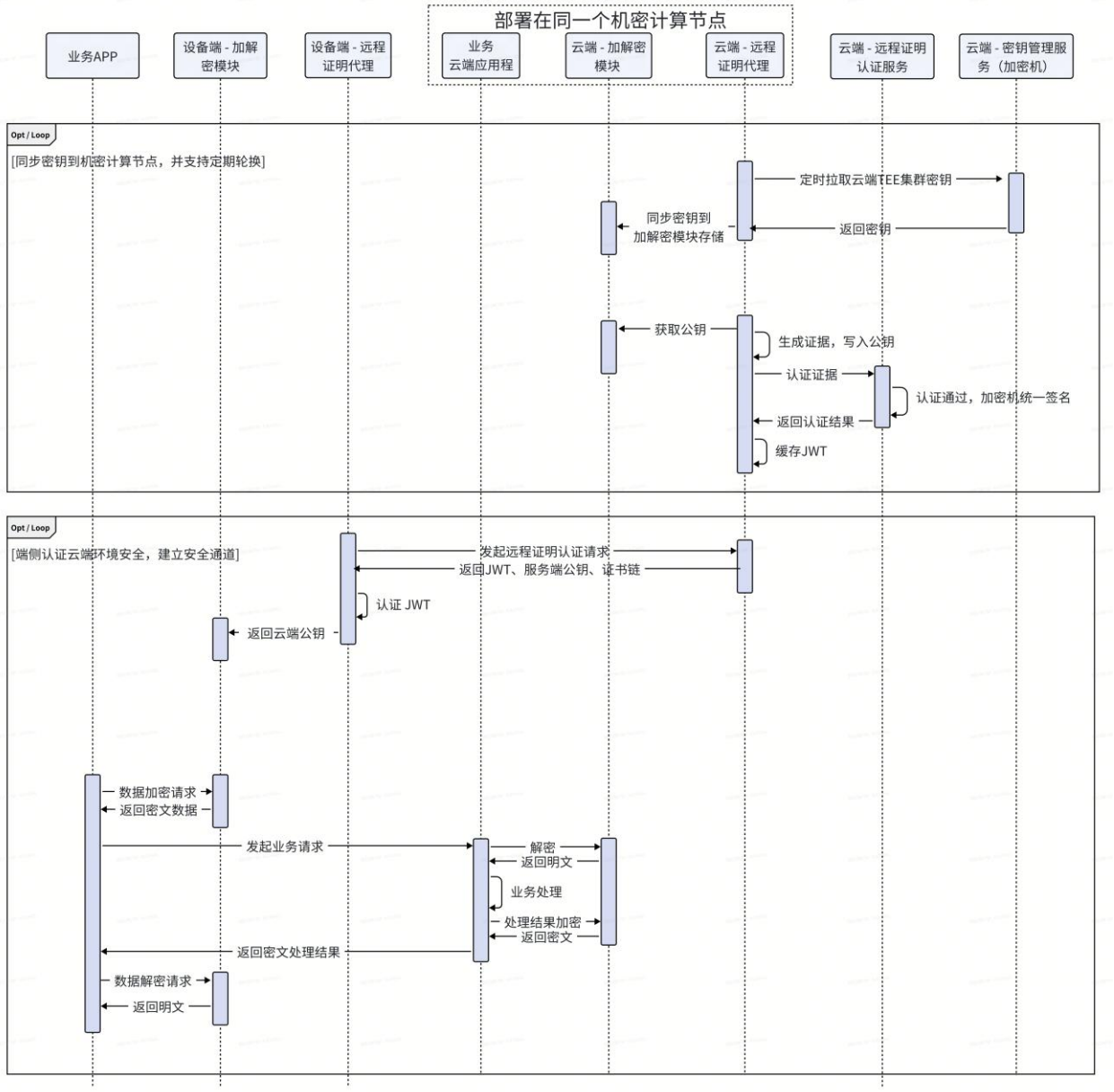


图 2　面向端云协同机密计算的远程证明执行流程

6　面向端云协同机密计算的远程证明功能要求

6.1　设备端

6.1.1　可信执行环境

基于硬件信任根的可信执行环境，宜为端侧设备提供一个隔离的运行环境，保护敏感数据和代码的机密性和完整性。

a) 硬件基础：宜基于硬件信任根的安全机制实现；
b) 功能要求如下：
   - 宜提供隔离、可信的运行环境，保障敏感数据与代码的机密性与完整性；
   - 宜在可信执行环境内强制部署远程证明代理与数据加解密模块，确保其运行不受外部进程干扰。

6.1.2 远程证明代理

设备端远程证明代理负责与云端的远程证明服务进行交互，获取云端证明报告信息并进行验证，确保端侧设备与云端的信任关系建立和维护，并完成密钥协商。

具体要实现的功能包括：

a) 应支持获取云端证明报告，并验证其真实性；
b) 应支持建立并维护端云间动态信任链，通过软件度量持续验证云端处于可信状态；
c) 应支持协商会话密钥供数据加解密使用。

6.1.3 数据加解密模块

采用非对称加密算法协商会话密钥，对设备端生成的数据进行加密处理，确保数据在传输和存储过程中的机密性。同时，负责解密从云端接收到的加密数据，为设备端的应用提供可用的数据。

6.2 云端

6.2.1 远程证明代理

云端提供的远程证明代理旨在简化企业业务系统的接入与集成，包括适配不同硬件厂商异构环境、自动生成远程证明报告，根据实际业务场景，可以直接复用云端远程证明代理周期性生成并缓存的机密计算认证结果，也可以触发云端远程证明代理生成新的机密计算认证结果，支持完成端云密钥交换。

具体要实现的功能包括：

a) 应支持证明报告的生成与验证；
b) 应周期性监控云端可信执行环境节点的运行时状态，验证硬件可信性和度量值完整性；
c) 应支持异常处理，远程证明报告认证失败时，立即触发节点隔离并通知安全运维中心。

6.2.2 远程证明认证服务

远程证明认证服务旨在兼容不同云服务厂商、多芯片的报告认证要求，通过统一的机制实现跨平台的安全验证。该服务能够对来自各个云环境的报告进行有效认证，确保其真实性和完整性，同时生成统一签名，以增强报告的可信度与可追溯性。

具体要实现的功能包括：

a) 跨平台认证：应兼容多云厂商报告格式，设备端厂商对远程证明报告作初步认证，认证通过后终端厂商签名并以 JSON Web Token 形式下发给端侧，报告应包括硬件制造商、系统完整性、信任根、系统配置、运行状态等内容，具体内容可参考附录 B；
b) 审计增强：宜记录报告哈希值及验证结果作为审计日志。

6.2.3 密钥管理服务

密钥管理服务提供全面的密钥生成和管理能力，确保业务在信息安全中的有效性和可靠性。

具体要实现的功能包括：

a) 应支持密钥的安全生成、存储和高效的身份认证机制，确保只有授权用户能够访问和管理密

钥；

b) 应支持密钥通过安全通道下发，访问控制基于 RBAC 模型和身份令牌认证，确保密钥能够可靠地传递给需要的应用和服务，从而保障数据的加密和解密过程的安全性；

c) 宜支持多租户密钥隔离存储。

6.2.4 数据加解密模块

采用非对称加密算法协商会话密钥，对云端生成的数据进行加密处理，确保数据在传输和存储过程中的机密性。同时，负责解密从端侧接收到的加密数据，为云端的应用提供可用的数据。

6.2.5 基线管理

基线管理模块负责定义、维护和校验所有机密计算环境的基准状态，确保硬件、固件、软件栈的配置符合安全标准。

具体要实现的功能包括：

a) 应支持对机密计算环境内的硬件、固件等 TCB 信息进行基线定义；

b) 应支持对机密计算环境内的工作负载进行基线定义；

c) 应支持对工作负载运行过程中加载的配置和数据进行基线定义。

6.2.6 策略管理

策略管理模块负责定义、存储、执行与审计所有与可信验证相关的远程证明安全规则。

具体要实现的功能包括：

a) 应支持对工作负载的启动过程进行策略定义；

b) 宜支持对敏感数据的访问和使用进行策略定义。

6.2.7 日志和监控管理

日志和监控管理提供必要的日志管理与监控能力，确保系统安全可靠运行。

具体要实现的功能包括：

a) 日志管理：

- 应支持记录关键操作，包括且不限于数据加解密、证明请求、密钥下发等；
- 应支持记录上下文信息，包括且不限于操作者身份、可信执行环境 ID、时间戳等。

b) 容器管理：

- 宜支持容器编排系统与可信执行环境集成，实现安全容器的弹性伸缩；
- 宜支持容器加密临时卷自动销毁。

c) 监控告警：

- 应支持监控硬件芯片健康及安全状态；
- 应支持监控云端服务存活状态；
- 应支持多级阈值告警。

7 面向端云协同机密计算的远程证明安全要求

7.1 设备端安全要求

要具备的安全要求包括：

a) 宜开启安全启动和完整性保护，基于硬件可信根建立信任链；

b) 宜支持可信执行环境隔离保护，敏感操作宜在可信执行环境内执行。

7.2 云端安全要求

7.2.1 云端计算环境安全要求

要具备的安全要求包括：

a) 应保证可信计算基最小化，宜仅依赖硬件可信根；
b) 应支持对硬件环境、运行时环境和工作负载进行度量；
c) 如采用硬件加速设备对数据进行处理，应具备同等安全水位的可信加速硬件，且支持远程证明。

7.2.2 日志安全要求

要具备的安全要求包括：

a) 存证日志内容应至少包括度量操作、中间状态、度量结果，并保证整个行为过程记录的完整性；
b) 存证日志应具备不可否认性，宜对存证日志附带数字签名；
c) 存证日志保存时间应不少于 6 个月，满足监管部门的审计要求；
d) 存证日志宜允许开发者查询历史证明结果对应的日志信息。

7.2.3 监控安全要求

要具备的安全要求包括：

a) 云端应持续验证对端环境和行为是否符合预期，并根据证明结果动态调整访问控制策略；
b) 监测行为异常事件后应触发异常告警，异常告警发生后端侧宜终止会话，云侧应将服务迁移到其他可信节点正常提供服务。

7.3 端云协同安全要求

7.3.1 协议流程安全要求

要具备的安全要求包括：

a) 应遵循 IETF RATS 架构模型进行远程证明协议设计；
b) 宜采用兼容 CBOR 结构化编码的证据格式，并利用 JSON Web Token 进行跨域认证，确保认证信息的安全性；
c) 宜保证不同机密计算环境度量范围的一致性；

7.3.2 身份与密钥管理安全要求

要具备的安全要求包括：

a) 应基于 X.509 证书建立传输信道保证云侧身份可信，宜采用身份证书体系保证端侧身份可信；
b) 应具备层级身份验证机制，宜对端侧环境、 云侧环境 、云侧工作负载进行认证；
c) 应对密钥生命周期进行管理，云端根密钥宜用基于硬件的保护机制保护，会话密钥应支持定期轮换。

7.3.3 数据处理安全要求

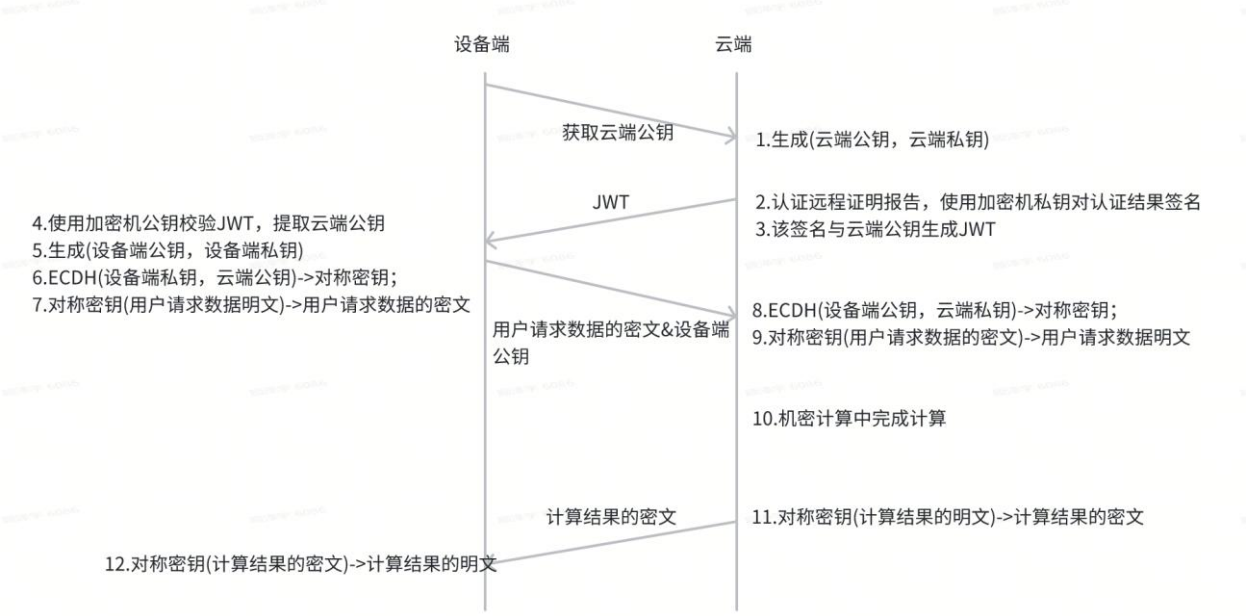
要具备的安全要求包括：

a) 宜基于远程证明的协商密钥进行全生命周期的数据流通保护，包括端侧数据预处理加密、云端解密计算、结果加密返回等；
b) 端侧和云侧的数据传输过程应采用 TLS 1.3 协议进行保护；
c) 敏感数据处理应在机密计算环境内进行，云端机密计算环境应启用内存加密引擎；

d) 敏感数据如需落盘应云端加密存储，并对相应的密钥进行安全管理，按照相关双方协商的销毁策略进行销毁。

附 录 A
（资料性）
端云传输业务数据使用的加密密钥的派生过程示例

派生算法可采用密钥协商、密钥封装等多种形式，例如ECDH、RSA、Kyber等算法，图A.1以使用ECDH算法为例进行介绍。



图A.1 基于ECDH算法的密钥派生过程示例

附 录 B
（资料性）
云端向端侧证明机密性的报告示例


```
{
  "sub": "VerifyCloudEndConfidentialComputing",
  "report_data":
"27883f5c3f8a2dc353f8634b0d263502faf563dacd02cae12218cf777b9148ed1f810ef57269458ff2295fe7
a69b9424e98a579e6bf1db3235b59b6ae8d43ef8",
  "user_data":
"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEquSbpe1DUJJ+rrkFFx2vdI50xD2fYRRmSg5nXkJsPqVQCx1QFdPG
Jaqc2DWUOPOs86sXfh2cm4bdzMJB41Z3yw==",
  "nonce": "KO23piLMWZFSNeDb1asNHg==",
  "biz_uuid": "test-48fb3d02ba5776a8a05012c76f63c860",
  "iss": "https://mipcc-attestation.engine.miui.com",
  "iat": 1765198547,
  "exp": 1765630547,

  "hw_manufacturer": {
    "vendor_id": "HW-VND-7A3F",
    "platform_model": "CC-PLT-2600X",
    "tee_type": "TDX-1.5",
    "security_version": 3
  },

  "system_integrity": {
    "boot_chain_verified": true,
    "firmware_hash": "a1b2c3d4e5f6...48hex",
    "os_image_hash": "f6e5d4c3b2a1...48hex",
    "app_enclave_hash": "9c8d7e6f5a4b...48hex",
    "measurement_method": "SHA-384",
    "secure_boot_enabled": true,
    "runtime_tamper_detected": false
  },

  "trust_root": {
    "root_type": "HW-RTM",
    "root_key_hash": "3e4f5a6b7c8d...64hex",
    "cert_chain_depth": 3,
    "attestation_service_id": "RA-SVC-0x01",
    "root_ca_fingerprint": "b7a6c5d4e3f2...40hex"
```

```
  },

  "system_config": {
    "memory_encryption": "TME-MK",
    "debug_disabled": true,
    "hyperthreading_disabled": false,
    "nested_virtualization_disabled": true,
    "min_tcb_version": "2025.03.01",
    "allowed_enclave_signers": [
      "SIGNER-ID-8F2A",
      "SIGNER-ID-4B7C"
    ],
    "network_policy": "EGRESS-RESTRICTED"
  },

  "runtime_state": {
    "enclave_status": "RUNNING",
    "uptime_seconds": 432047,
    "last_attestation_epoch": 1765198540,
    "active_sessions": 12,
    "memory_utilization_pct": 34.7,
    "anomaly_flags": [],
    "heartbeat_seq": 88421
  }
}
```

电信终端产业协会团体标准

面向端云协同机密计算的远程证明技术要求

T/TAF 347—2026

*

电信终端产业协会发布
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn