


ICS 33.050

M 30

团 体 标 准

T/TAF 082.1-2021



网络设备密码应用技术要求 通用要求

Cryptography application technical requirement for network devices—
Common requirements

2021-01-18 发布

2021-01-18 实施

电信终端产业协会 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 网络设备密码应用技术要求	2
4.1 软件/固件安全	2
4.2 身份鉴别	2
4.3 访问控制	2
4.4 网络通信安全	2
4.5 数据安全	3
4.6 计算安全	3
4.7 物理安全	3
4.8 性能要求	3
附录 A（资料性）重要数据说明	4
参考文献	5

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。

本文件是网络设备密码应用技术要求系列标准之一，该系列标准结构预计如下：

《网络设备密码应用技术要求 通用要求》

《网络设备密码应用技术要求 路由器设备》

《网络设备密码应用技术要求 交换机设备》

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。

本文件提出各类网络设备密码应用技术通用的、基本的安全要求。

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：中国信息通信研究院、华为技术有限公司、中兴通讯股份有限公司、新华三技术有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：张治兵、张亚薇、秦书锴、陈鹏、周继华、童天予、刘为华、吴荣春、叶郁柏、万晓兰、薄菁、吴萍。



引 言

为推进《网络安全法》的落地实施，本文件提出网络设备密码应用技术应满足的通用安全技术要求。

密码技术是网络安全的核心技术，是信息保护和网络信息体系建设的基础，是保障网络空间安全的关键技术。本标准属于网络设备密码应用技术安全要求系列标准中的通用标准，对各类网络设备，除满足本标准要求，还应满足相应设备的密码应用技术安全标准要求。



网络设备密码应用技术要求 通用要求

1 范围

本文件规定了网络设备在软件/固件安全、身份鉴别、访问控制、网络通信安全、数据安全、计算安全、物理安全与性能等方面的密码应用技术的通用要求。

本文件适用于在我国境内销售或提供的网络设备，也可为网络运营者采购网络设备时提供依据，还适用于指导网络设备的研发、测试等工作。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GB/T 37092—2018 信息安全技术 密码模块安全要求

3 术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

网络设备 network devices

网络设备指具备连接网络功能的实体（不包含消费类终端产品）。

3.2

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.3

解密 decipherment/decryption

对密文进行密码变换以产生数据的过程。

3.4

密钥 key

控制密码算法运算的关键信息或参数。

3.5

保密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.6

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.7

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。

3.8

重要数据 important data

重要数据包括认证口令、管理指令、设备信息等，具体参见附录B。

4 网络设备密码应用技术要求**4.1 软件/固件安全**

网络设备：

- a) 可使用密码技术保证软件/固件保密性
- b) 可使用密码技术来保证固件/软件完整性
- c) 可使用密码技术保证软件/固件抵御常见的攻击，如反编译、重打包等
- d) 远程升级时，应使用密码技术保证固件/软件升级包的完整性与身份校验

4.2 身份鉴别

网络设备：

- a) 应使用密码技术对访问控制实体进行身份鉴别，可使用密码技术进行双向身份鉴别
- b) 可使用密码技术对口令认证中身份鉴别信息进行加密
- c) 可使用密码技术对口令认证中身份鉴别信息的传输进行加密
- d) 可使用密码技术来抵御常见的重放攻击

4.3 访问控制

网络设备：

- a) 可使用密码技术保障访问控制功能安全性
- b) 可使用密码技术保证访问控制信息的完整性
- c) 可使用密码技术保证访问控制信息的不可否认性
- d) 可使用密码技术来抵御特定的越权攻击，如会话劫持等

4.4 网络通信安全

网络设备：

- a) 应支持使用密码技术建立可信信道/可信路径
- b) 应使用密码技术保证通信传输过程中重要数据的保密性
- c) 可使用密码技术保证通信传输过程中重要数据的完整性
- d) 可使用通信数据加密后再传输的方式保证信息不被泄露
- e) 应使用密码技术保证在非安全通道传输时重要数据的保密性与完整性

4.5 数据安全

网络设备：

- a) 应使用密码技术保证重要数据在传输过程中的保密性
- b) 可使用密码技术保证数据在传输过程中的完整性
- c) 应使用密码技术保证重要数据在存储过程中的保密性
- d) 可使用密码技术保证数据在存储过程中的完整性
- e) 可使用密码技术保证设备抵御常见的攻击，防止密钥等重要数据泄露，如计时攻击等

4.6 计算安全

网络设备：

- a) 应使用符合GB/T 32915-2016标准的随机数生成器，显著性水平指标参考GM/T 0005-2012
- b) 可使用可信计算技术建立可信计算环境
- c) 可使用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证
- d) 以上使用的密码技术应使用安全强度较高的密码算法，不应使用md5、SHA1、DES等

4.7 物理安全

网络设备采取下列技术保护加密模块：

- a) 应具有防止电磁信息泄露与抗电磁干扰能力
- b) 应具有预防线路截获导致设备无法正常工作或重要数据泄露的能力
- c) 应具有抗调试的能力，如关闭调试接口，或在调试时不能泄露私钥等重要数据
- d) 可使用相关技术保证设备抵御常见的侧信道攻击，如缓存攻击、计时攻击、电磁攻击、基于功耗的旁路攻击等

4.8 性能要求

网络设备：

- a) 应具有能够运行安全强度较高密码算法的相关性能，如SHA256/SM3、AES128/SM4等算法
- b) 应具有在运行高强度加密、解密算法时不会出现因负载过高而造成不能正常提供服务的情况
- c) 应具有硬件密码计算功能，能够满足高强度加解密算法的性能要求

附录 A
(资料性)
重要数据说明

重要数据包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等。



参 考 文 献

- [1] 信息安全技术 信息系统密码应用基本要求（征求意见稿）
 - [2] GB/T 37092—2018 信息安全技术 密码模块安全要求
 - [3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
 - [4] GB/T 32915—2016 信息安全技术 二元序列随机性检测方法
 - [5] GM/T 0014—2012 数字证书认证系统密码协议规范
 - [6] GM/T 0005—2012 随机性检测规范
-



电信终端产业协会团体标准
网络设备密码应用技术要求 通用要求

T/TAF 082.1—2021

*

版权所有 侵权必究

电信终端产业协会印发

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